Pinto Next AF/LCD

Users' Manual 1.6

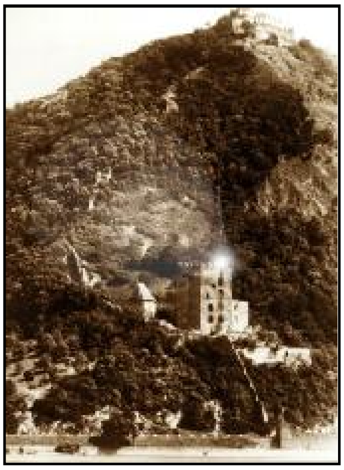
Table of contents

1 Introduction

1.1 What is FSO?

FSO is free space optics provides point-point broadband communications using Laser Light as the transmission medium.

FSO is a state of art data communication method which is based on a very old communication solution. Ancient Chinese developed a protection system against the Mongol tribes, building watchtowers within the line of site to other towers. And as soon as the towers saw some hostile sign on the horizon they use they shield to reflect the sun to the remote towers. In this way the area could be prepared against the attack in a very short period of time.



In the ancient times for this communication use the mirror as a transmitter and the sunlight was the light source, and the receiver was the remote guard's eye. This basic signalling method was developed later into up communication device which used „line coding". This allowed the guards to tell the number of enemy, or the direction they are coming from.

Current **FSO** systems use a laser-diode as a light source, and a receptor diode (photo diode) to receive the signals coming from the laser diode from the transmitter side. But the basic elements are still the same: line of site between the communication nodes, and individual line coding. It is all about performance. **GeoDesy FSO** offers **FSO** systems with the highest power budget available on the market.

1.2 Why is it important?

Because of in the ancient Chinese times, the rain, the fog, or even the cloudy weather, could impact the operation of the whole system.

In the **FSO** units, comprising light source and receiver the cloud problem was solved, but development conditions still can impair performance. To go throw the rain, the fog, or snow you need more and more power to be seen from the remote side. Achievable power levels are limited by a number of factors including eye safety.

In this way there is no other choice to see more than „training the eye". Making the receiver more and more sensitive to sense delight emitted from the remote side. **GeoDesy FSO** offers high transmit power and also very hard receiver sensitivity. These two factors combined to provide one of the best performing **FSO** systems on the market today.

To meet the demands for every higher bandwidth, **GeoDesy FSO (Europe) Limited** continues to invest heavily in research and development with the newest product line which offers Gigabit speeds being launched.

This manual describes the **GeoDesy FSO Next** series of free space laser transmission system.
The **GeoDesy FSO Next** product range offers cost effective reliable free space laser transmission for two Mbps up to 1000 Mbps data to the air, where a clean line of site is available. It delivers the most effective point-to-point connection between computer networks or telephone exchanges.
No need for installing cables, no rental costs, no licensing requirements.

Ideal for urban areas or city centres, where the use of these lines are expensive. Suitable for factories or industrial environments where high noise level can interfere with the transmitted data. The best choice to make a connection across rivers and other natural or artificial obstacles, where cable is not available.

The transmission technique used in the **GeoDesy FSO** devices provides transparent and wire-speed data transfer with virtually zero latency. Because they use infrared light as the transmission medium, **GeoDesy FSO** system do not require frequency licenses and the transmission is not effected by electro-magnetic or radio-frequency interference. Basically the **GeoDesy FSO** link can be considered as a virtual fibre in the air, which ends in real fibre optic cable at both ends.
Our product is built using high quality components for operation in even the most adverse conditions.

Metal housing gives robust, waterproof environment for the electronics.
The shield protects the device from direct sunlight and provides extra air isolation.
The **GeoDesy FSO X** systems comprise two laser-heads and the two indoor interconnection units (OIU) - one at each end. The interface connections are housed in the outdoor unit together with the PSU of the system.

Best practises were employed in cost engineering throughout the development of **GeoDesy FSO**.

1.3 Optical Free-space Transmission

The principle used in free space laser transmission is very similar to the one is used for fibre optic transmission. The difference is while fibre optic devices use electronics and optics optimized for transmission to the air. Also one can observe to the similarity in the transmission properties. No galvanic contact, no ground-loops, no need for surge protection, noise immunity, long distances, high bandwidth.

What makes it unique – and difficult to design – is that it does not require any transmission medium like fibre or copper, but it has to cope with the dynamically changing parameters. For instance while the attenuation of an optical fibre is constant, the attenuation of the atmosphere between the laser units can change dramatically (depending on the weather conditions).
The laser-heads are usually placed on top of building, where the clean line of site is guaranteed and the beam cannot be interrupted.

In the head the incoming signal is amplified, encoded, and then drives the laser-diode. The transmitter optics assures the proper beam shape and controls the beam divergence. The receive optics perceives and directs the transmitter signal to the photo diode. The diode converts it back into electrical, than it is decoded, amplified and converted.

There are several things that can influence the quality of transmission. We can classify those factors into three main groups.
System conditions - transmitting power, transmitter's wavelength, beam divergence, receiver optics diameter, receiver sensitivity, parameters of optical system and casing. These parameters determine the system's characteristic at a certain distance and are controlled by system design and factory set up.

Weather conditions - molecular absorption, particle scattering and turbulence. These elements have great effect on the operational conditions of the system. We do not have very much influence on them; proper product selection can eliminate the undesirable effects.

Environmental conditions - building movements, direct sunlight, refractive surfaces. These are also key factors related to the installation sites and can be controlled by appropriate site survey and system installation

1.4 Typical applications

Most typically the **GeoDesy FSO Next** products are used to interconnect LAN-s. The system is protocol transparent, thus other applications also can be taken into consideration. Appropriate interface converters are needed and system bandwidth must be matched for that.

Here we collected some circumstances, where the deployment of the **GeoDesy FSO** is the most adequate as a cost effective solution.

Those are:

Areas with natural or artificial obstacles

Where cable is actually not an alternative, like across rivers or railways or in rugged terrain.

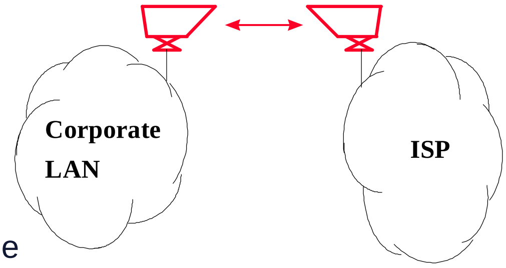
Urban areas

Where only leased lines are available with limited speed, and high rental cost. With GeoDesy FSO links you can establish on line LAN-to-LAN connections.

Industrial areas

Where you have noisy environment with high EMI or RFI. Factory buildings, airport objects can be connected through laser link.

ISP connections



Where high bandwidth is required. ISP’s can offer high-speed links to their customers or trunks can be established between ISP’s instead of expensive leased lines.

2 Interfaces for the X Series

2.1 100Mbps TP interface

The **GeoDesy FSO X PoE** series products are designed to provide easy-to-use and cost-effective solution for interconnecting Local Area Networks. By utilizing standard Category 5 cable and using standard IEEE802.3af interface the deployment of the system is easier than ever before. The transparent and wire speed data transfer together with virtually zero latency assures the easy integration of the system in all environments.

The **X PoE** systems should be considered as repeaters in the network. So the installation distance between the head and the network device is 100m. The distance on a back to back site is maximum 5 meters, between the heads without signal regeneration.

The **X PoE** systems connecting to the network with an RJ 45 cable which provides the power required for operation and the data. The system requires IEEE 802.3af Power over Ethernet switch or power injector. The power consumption suits to the standards described in the standard. Also provides fast and easy connection for the management system for more details please see the chapters below. The system is certified **Class 1M product**, this way 100% eye safe.

3 Sites of installation

3.1 Key factors of operation

There are four key issues that the site survey has to shed light on. Proper system operation cannot be guaranteed without satisfying all of the four requirements.

Clear line of sight - The entire optical path between the two ends must be free of any obstacles. It not only means that one has to see the other side, but other possible sources of disturbance should also be taken into consideration. For example there might be turbulence above the roofs and other constructions, and this can cause fraction or scattering of the beam or snow accumulation on roofs too close to the beam can influence or even interrupt communication.

Solid mount surface - is the key for long-term operation. Since the diameter of the beam is limited, it is extremely important to mount the unit on a stable structure with the possible smallest movement. This way the receiver of the remote unit cannot get out of the beam due to the movement of the opposite head.

East-West orientation - although the receiver optics are equipped with optical filters to protect the receiver diode from the effect of undesired light sources, direct sunshine can cause saturation of the diode. This prevents the system from working properly for several minutes a day at certain times of the year. In most cases this effect can be avoided by careful selection of the mounting spot.

In order to comply with the requirements of the successful installation - including the discussed four key factors and other criteria - the following matters should be taken into consideration.

3.2 Preferred installation sites

All buildings and constructions have a certain movement of their own. It's determined by the structure and material of the building. Metal structures can shift or twist due to temperature changes. Wooden construction can expand or shrink with any changes in humidity. Give preference to concrete or brick buildings. On the other hand high structures like towers, skyscrapers or poles are always subject to movement. Mount the support frame to walls of the building or near corners, as they are the most stable spots. Use appropriate consoles for wall mounting. If a stand is used on the top of
building, secure it directly to the ceiling or to the concrete cornice wherever is possible. Do not fix stands to insulating materials as they can slowly sink under the weight of the unit and with temperature changes. Big chimneys and smokestacks may look stable, but as their inner temperature varies they can also move. Vibration caused by heavy traffic, trains and elevators etc. may slowly move the system out of its specified direction. Another important consideration is to provide enough space for alignment and to have the potential for future maintenance. Consider that the support frame is usually heavy, so the selected spot should be easily accessible.

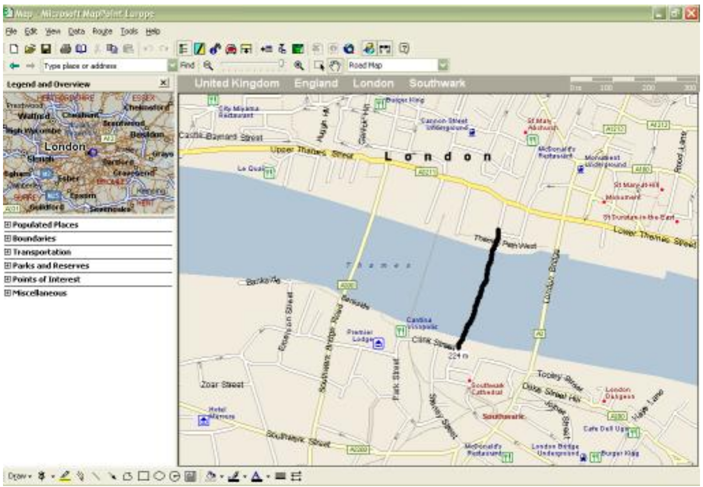
Preferred installation sites	***Pay attention to***	***Avoid (*)***
Concrete wall	Behind window	Soft materials
Brick wall	Old constructs	Chimneys
	Microwave towers	Wooden constructs
		Metal masts or Frames
		Hidden heat isolations, like Styrofoam

(*)
In cases where installations are listed under "AVOID" cannot be avoided than special mounting accessories to be designed and special installations must be used.

It is not only the building that has to be solid, but the support structure too. Antenna poles and security camera holders are not suitable for the **GeoDesy FSO** units.

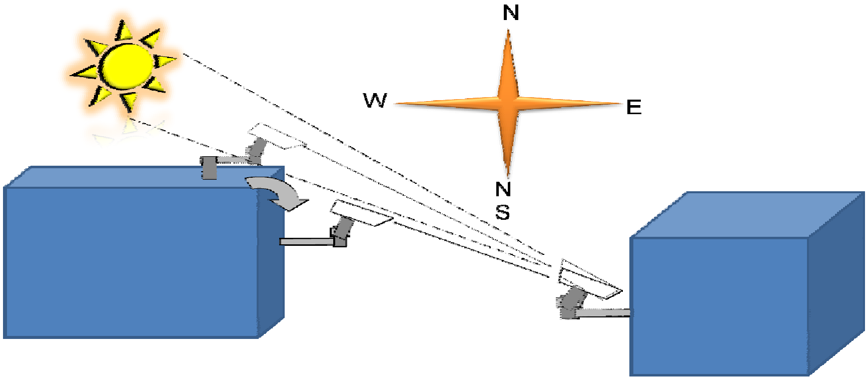
3.3 Distance measurement

Because the units were designed, and calibrated for certain distance operations the higher distance will decrease the availability. GeoDesy FSO pre-calibrates and pre-tests every unit shipped to the customer. To ensure that the unit you are about to buy fits to the needs, the first step is to measure the distance. The best way to measure it is by GPS (Global Positioning System), these units are accurate enough to determine the distance between two points. For more details please refer to the GPS manufacturer handbook. Also there are several other ways to measure the distance. If you know the exact address you can use mapping software like MapPoint or Auto route.



3.4 Direct sunshine

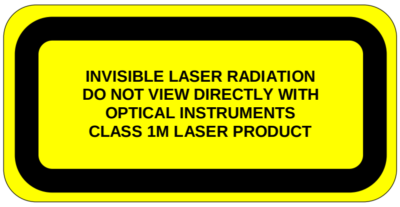
To prevent the sun shining directly into the receiver optics, first one has to determine the orientation of the link. Try to avoid East-West orientation wherever it is possible. Examine both sides of the link at sunset and sunrise and find a position where the sun cannot get behind any of the heads. Be aware that the path of the sun is changing throughout the year.



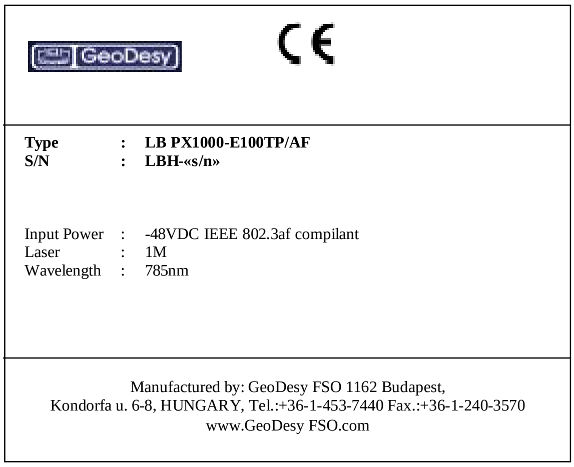
4 Eye safety

There are no two installation spots of the same kind, the buildings or structures, the available space and the accessibility of the place will be different in each case. Nevertheless, as a general rule it is very important to select the installation site so that nobody can look directly into the transmitter. For this reason place the head either so high (on the side wall of the building) or so close to the edge of the building (on a parapet on the rooftop) that no person can approach it accidentally and can get into the beam path. Set up barriers if necessary and put warning signs at prominent places.

The laser heads are provided with all labels and hazard warnings required by the laser standard. There are warning labels on both the left and right side of the protective cover next to the optical window and there is a warning and an informative label on the rear side of the laser head.



INVISIBLE LASER RADIATION
DO NOT VIEW DIRECTLY WITH
OPTICAL INSTRUMENTS
CLASS 1M LASER PRODUCT



GeoDesy CE

Type	**:**	**LB PX1000-E100TP/AF**
S/N	**:**	**LBH-«s/n»**
Input Power	:	-48VDC IEEE 802.3af compilant
Laser	:	1M
Wavelength	:	785nm

Manufactured by: GeoDesy FSO 1162 Budapest,
Kondorfa u. 6-8, HUNGARY, Tel.:+36-1-453-7440 Fax.:+36-1-240-3570
www.GeoDesy FSO.com

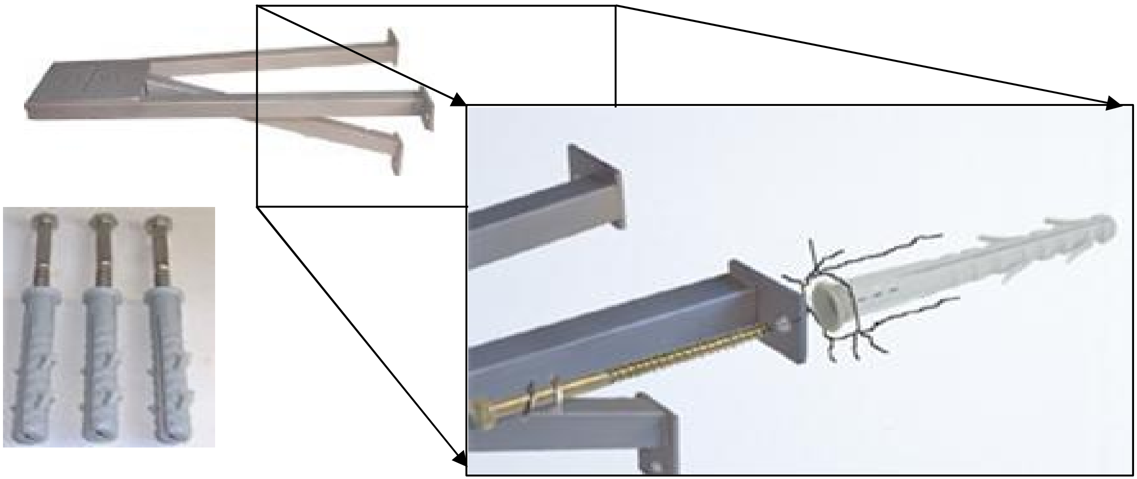
5 The mounting bracket

In the following chapter you will find detailed description of the bracket fastenings.

5.1 Mounting brackets for the X Series

GeoDesy FSO provides the mounting bracket and all the necessary components for **X** series units. A simple fixing technique of this bracket can be seen on the following figure, required tools are as follows:

- drilling machine
- 10 mm wrench



Bracket sizes:

Length:	463mm
Leg Width:	263mm
Head Width:	130mm
Drill size:	10mm wall drilling

Installation steps:

- Place the bracket on the wall
- Mark the wall with a permanent marker
- Use your 10mm wall drill to drill all of the holes into the wall
- Clean the holes
- Place the wall-plugs into the holes (please note that some times you need to use hammer to put the wall-plugs into the hole, if you have to please be careful not to break the wall-plug)
- Place the bracket to the wall an line it up to the holes
- Put the screws into the wall-plug through the hole on the leg of the bracket (please see the figure above)
- Tighten up the screws

Packet list for the bracket:
3pcs 8x110 screw for bracket fixing

3pcs 8x100 plastic wall-plug for bracket fixing

2pcs M6x90 bolt Head fixing
3pcs M6x25 screw Head fixing
3pcs M6 bolt head fixing
6pcs 6mm spacer bracket and head fixing
6pcs 6mm spring spacer bracket and head fixing

6 System installation

6.1 On the table test

Warning! Do not look either into the transmitter or the receiver optics because at this distance even the reflected laser beam *can* be dangerous to your eyes. Operating the system on much shorter distance than presumed originally can cause saturation or even permanent damage to the receiver. Always use optical attenuators for this kind of test.

The on-the-table test needs careful planning and careful use during the test period. The units should be placed at about 2 m distance from each other with optical windows facing one another. Put an appropriate optical attenuator (Attenuating foil or cardboard with several small holes) between the heads. Make all the necessary connection as described below to connect your network equipment (computer or protocol analyzer) to the heads and power up the units. Turn ON the Poe injector and check if the power LED is ON on the head.

You should be able to align the units without any tool and get full received level on the signal strength LED's. Make sure that the "Saturation" indicator is OFF. Adjust your attenuators if necessary to avoid saturation of the receivers.

Please note that at this short distance, specially the longer distance links can reflect to the remote site or even to the same head. If you experience full receiving level, with no traffic throughput, in that case try to move the heads slightly units out of the reflection zone.

Please also take in consideration that the laser beam is concentrated and in such a short distance can harm your eyes, every time you test the units on short distance, do it with extra care. Never look into the sighting device if the remote laser is turned on. We strongly suggest to double check the power connection before you turn on the device. Handle the power connection with extra care. Safety first.

After obtaining the desired received level, check the data connection between devices. Using computers or appropriate testing devices.

On the table tests are perfect for troubleshooting (If there is a transmission problem, check the status of the connecting devices (e.g. Link signal or cable polarity) and cables.) in a controlled area. If you experience some problems during the test, please try to test the connected equipments with a direct connection.

6.2 AF adjustment method

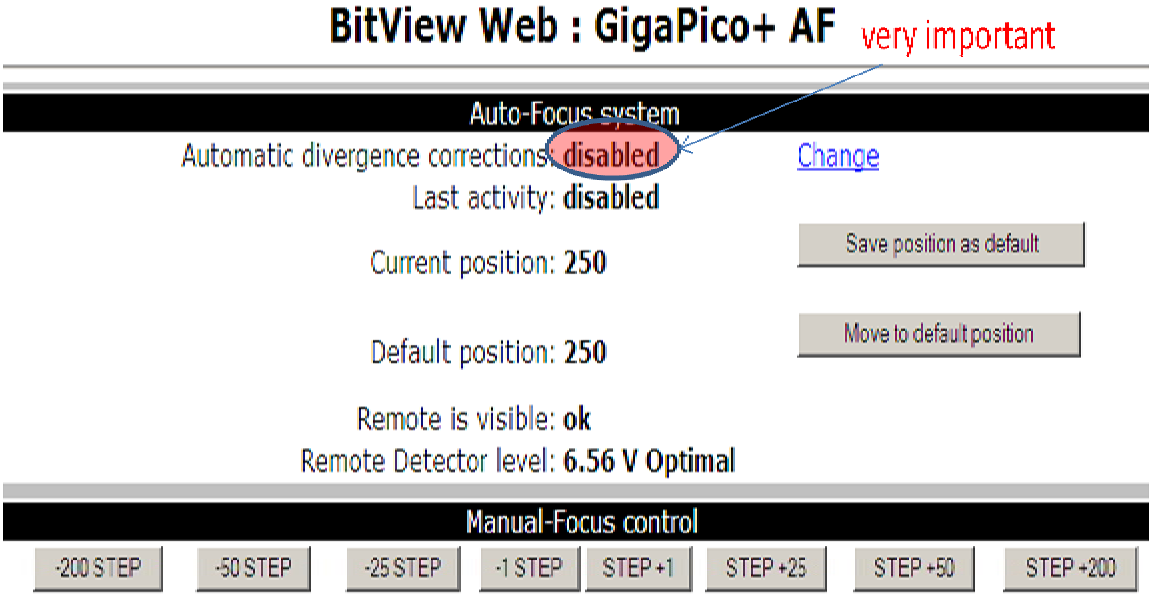
What is AF after all? AF stands for Auto Focus. **Geodesy FSO Pinto Next AF** is equipped with the lates innovation from Geodesy. An automatic focusing control system. The system is capable of changing its beam divergency depending on the changes of the environment. In the case if the weather gets bad, the system will decrease the beam size, to concentrate the distributed beam power, to ensure more stable operation.

IMPORTANT! Auto focus adjustment does not work if there is no remote level! Remote connection required for the Auto focus adjustment.

The installation of the **Pinto Next AF** is pretty much the same as the standard system installation. To make sure that the AF system won't kick in during the alignment, ensure that the AF is set to disabled, which is the factory default.

The default settings of the Auto Focus (AF) laser heads is manual mode (disabled). The factory beam divergence is set for 750m, this way the alignment of the system will be easy on every installation distance.

Please do not change the setting of the AF laser heads to auto focus when there is no connection between the two heads.



BitView Web : GigaPico+ AF

very important

Auto-Focus system

Automatic divergence corrections: disabled

Last activity: disabled

Current position: 250

Default position: 250

Remote is visible: ok

Remote Detector level: 6.56 V Optimal

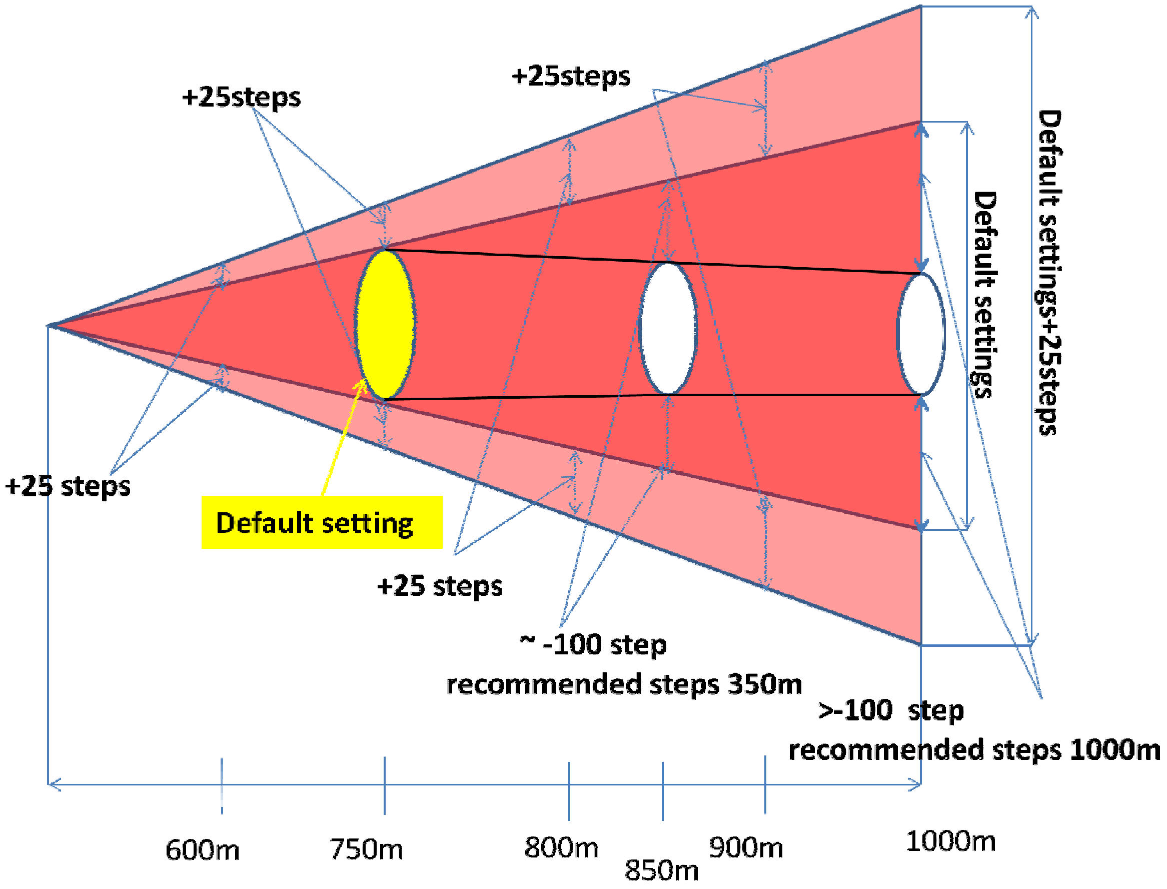
Manual-Focus control

Alignment steps

1. using the crosshair align the units into a roughly aligned position. Please note that the alignment scope will not be able to provide with a perfect alignment, this will have to be done using the fine alignment screws referring to the received level screen on the LCD panel.
2. using the fine adjustment screws on the alignment base set the units to the highest received level possible. (for further details on how to perform the fine adjustment refer to 6.2.1 and 6.2.2 chapters)

Default distance setting of all **Pinto Next AF** laser heads for 750m. As you can see in below sketch, “+25 STEP” equals ~ 2 cm larger laser beam over 100 meters.

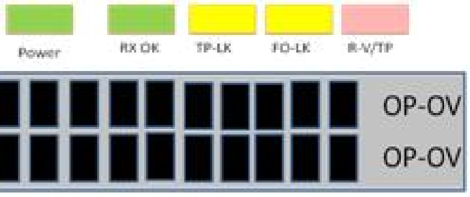
For example, if you would like to install the laser heads over 350 meters than you will need smaller beam size to reach bigger distance (compared to the default 750m), so click on “-100 STEP” which will make the laser beam narrower and will be proper for 850m. While clicking on the “STEP” buttons please check the remote received level on the laser head.



Please perform the same operation on the other side.

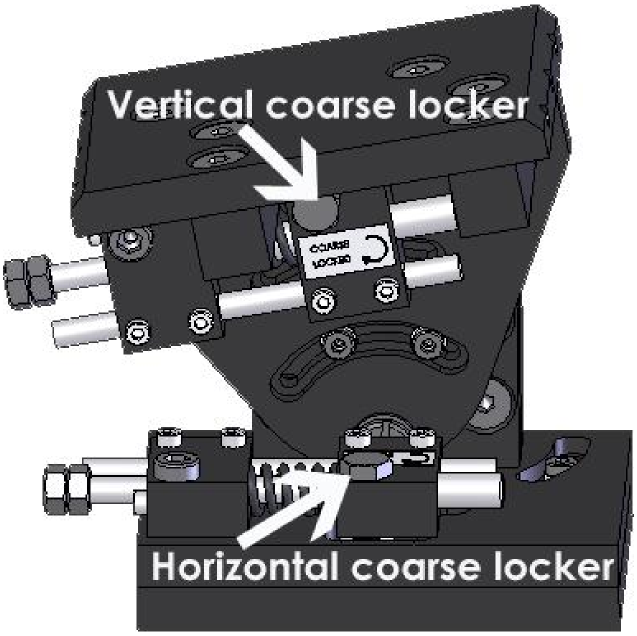
3. After we have got the proper level, please click on “Save position as default” button. As you have clicked on the “Save position as default” button the laser heads will enable the AUTO FOCUS mode (enabled). The equipment will automatically improve the remote level to the most ideal position.

Alignment of the **X series**



The first step after the unit was placed to the bracket, and turns the units facing each other.
On the back of the receiver you can find the LEDs for the local received level and the remote received level. This help will be very useful because as soon as you have received – which is very easy to achieve – you can see the effect of your local sides movement to the other side. For further information please check the *Meanings of the LEDs* chapter.

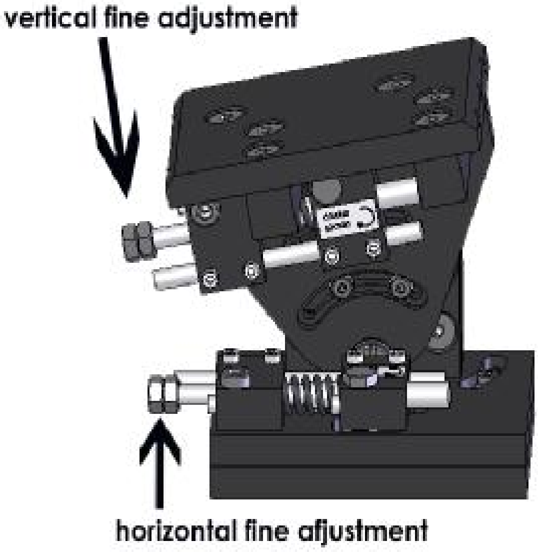
6.2.1 How to use the alignment base



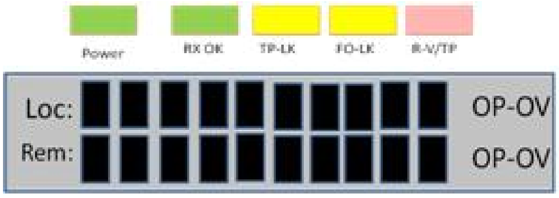
1. Loose the Coarse locker on the horizontal as well as on the vertical side with a 10mm spanner
2. Move the head left - right up down you should use the built in telescope to lit up a few LEDs on the remote end.
3. When you have lined the unit up to a rough position lock the coarse locker with a 10mm spanner.
4. Repeat step 1-4 on the remote end.
5. On the bottom of the unit you can find fine tuning screws one for horizontal and one for vertical.
6. No tightening is needed on any other screw than the coarse locker.

6.2.2 Fine tuning

1. Site A start moving the laserhead with the horizontal fine adjustment screw by looking at the Remote end received level
2. Using the fine adjustment screws, lighten as many LEDs as possible
3. Repeat step 1-2 on Site B.
4. If necessary try step 1-2 on both sites again.



6.2.3 Meanings of the LCDs



Power:
The head is powered up.

RX-OK:
Received beam is good for communication.
TP Lk:
Copper link between the head and the Network equipment.
R-LS:
The recived signal form the remote end is modulated and .
RV/T-LS:
Remote end is visible for the management system and there is TP connected to remote end – same as TP-Lk but displays it on the remote end.
Top Level LEDs:
Local Received level
Bottom Level LEDs:
Remote Sites Received level
10th LED:
The 10 th LED has three functions showing that the recived level reached its optimum this is green, it maximum it is yellow or the receiver got saturated and this is red

Please press the button and look at the LCD scren!

1. screen

Loc (local level): Local Received level
Rem (remote level): Remote Sites Received level
Op-optimal
Ov-overload

2.screen

HeadSN: Laser head serial number.
0000001

3.screen

Temperature
TT°C

4.screen

-AF mode position manual 000
-AF mode auto
Here shows that the auto fucus with is enabled or disabled.

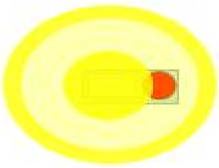
5.screen

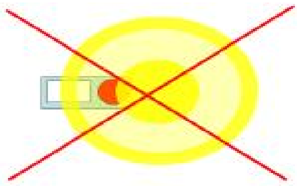
tech@geodesy.hu

Note: Geodesy FSO shall not be responsible for any failures from improper handling of the device. If any other screw than the coarse lockers or the fine adjustment is moved, might decrease the stability of the installation.

Trick for the reliable alignment

Please note that the beam has a powerfull ring on the side of the head and easily can be set to this ring but this is far not as big as the core part of the beam. So every time you have an alignment please make sure that when you see the maximum LED s or a relativly high received level. Keep on moving to determine where the core part of the beam is. This can be done easily by looking at the received level you will see that the received level moves up then it will start move down than up again. During this time you just had the head moving into one direction. If you have any doubt on how to do the alignment please contact your distributor for further help. Or contact GeoDesy FSO technical support.





6.2.4 Connecting to your Network

PoE 802.3 af connection.

PoE system is connected to the network via one twisted pair cable. This provides the power and the data for the GeoDesy FSO PicoX laser head
The unit has connection for the management on the bottom of the Laser unit.
Please see the connection below.
This is the standard IEEE802.3af connector layout.

1. Orange/White	TX+
2. Orange	TX
3. Green/White	RX+
4. Blue	+VIN
5. Blue/White	+VIN
6. Green	RX-
7. Brown/White	-VIN
8. Brown	-VIN

7 Management

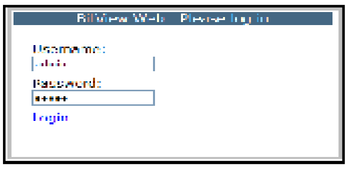
7.1 Features

The **Inband** network-monitoring unit is a newly developed highly featured monitoring for GeoDesy FSO manufactured laser links. This high quality equipment allows the user to monitor the link statuses such as detector voltage transmitter status, and many other features of the Laser link. Nevertheless, this chapter is intended to describe the usage of this network monitoring, and its connection and relationship with the GeoDesy FSO laserheads.
The Monitoring system is a standard feature in the PicoXp and PintoXp systems. For PicoXs and PintoXs it is an optional and has to be activated. After the activation was purchased, with the invoice number, and the device serial number contact GeoDesy FSO technical support, for activation code. For further information check Activation chapter.

Inband monitoring is providing information about

Login Screen and password

The GeoDesy FSO unit arrives with preset values. Such as user name and password. We strongly recommend you to change the password after the unit was installed. The default username is admin, and the password is admin. If you forget your password contact technical support to receive your fail-safe password.



BitView Web - Please log in

Username: admin

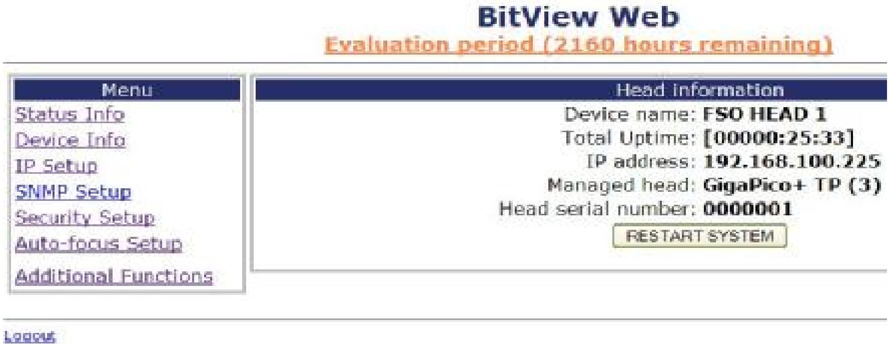
Password: *****

Head information screen

The head information screen is the main navigation panel through this screen you will be able to navigate into the submenu, of the monitoring system.

Device Name: displays the name of the device. Individually can be changed

Total Uptime: Diplays the lapsed time from the last boot of the device



BitView Web

Evaluation period (2160 hours remaining)

Head information

Device name: FSO HEAD 1
Total Uptime: [00000:25:33]
IP address: 192.168.100.225
Managed head: GigaPico+ TP (3)
Head serial number: 0000001

IP address: Displays the IP(Internet Protocol) address of the device which must be a unique identifier in the

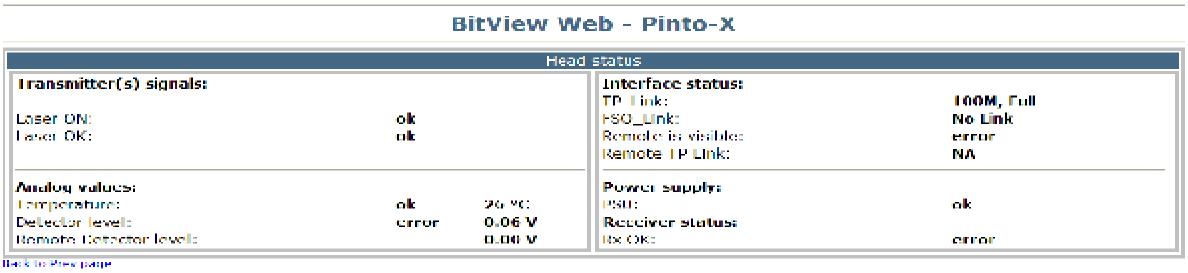
network.

Managed head: displays the managed head type.

Head Serial Number: This is the head serial number and during the Activation process we will ask for this number.

Status info screen

Clicking on the Device Setup you will enter the main status information screen, which will give you good summarized information of the device, such as status information of the transmitters, detector level, or temperature values.



BitView Web - Pinto-X

Head status

Transmitter(s) signals:			Interface status:	
Laser ON:	ok		TP_Link:	100M, Full
Laser OK:	ok		FSO_Link:	No Link
			Remote is visible:	error
			Remote TP Link:	NA
Analog values:			**Power supply:**	
Temperature:	ok	26 °C	PSU:	ok
Detector level:	error	0.06 V	**Receiver status:**	
Remote Detector level:		0.00 V	Rx OK:	error

Back to Prev page

Laser ON: Transmitter transmitts

Laser OK: Transmitter works properly, transmitts and the transmitted signal is valid.

Temperature: ambient temperature inside the device. These units were designed for extreme conditions and should not have any problems under -20C to 70C. In fact the unit is emitting some heat so the temperature displayed is not the air temperature outside the head. For example the temperature can be -10C outside but in the device it wont go below -1 or -2. The value will display error depeding on the setting was done device setup. There is no default value for this setting, only a suggested value, which is 60C.

Detector level: shows the local heads received level. In volts, the maximum is 7 volts and the minimum is 0.2 volts. The value will display error depeding on the setting was done device setup.

Remote Detector level: this value is dispalyed form reception of the remote head. The maximum is 7 volts and the minimum is 0.2 volts.

TP_Link: displays that there is connection over the TP cable.

FSO Link: displays that there is valid signal received from the remote end.

Remote is visible: this status information is a good information about the connection over the two laserheads if this status is OK that means that there is data transferred over the link.

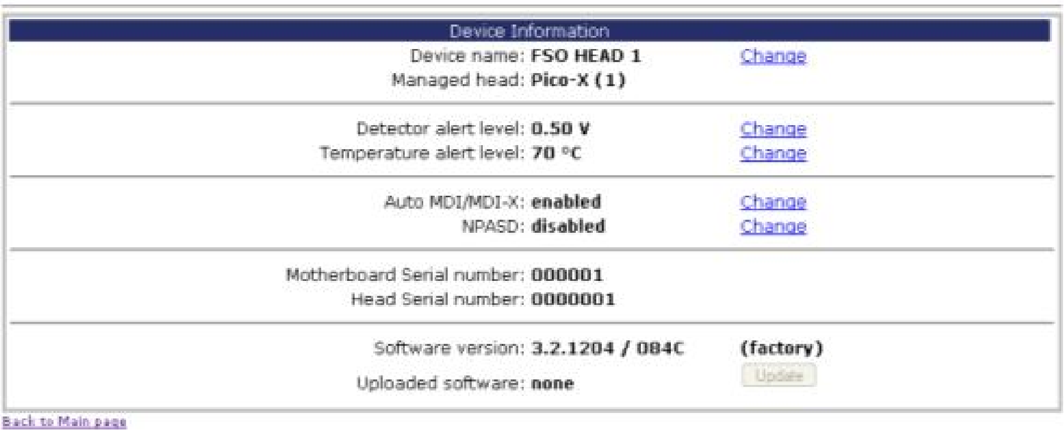
Remote TP Link: shows that whether the remote end is connected into the switch and the TP interface is available.

PSU: The PSU of the device is sending the OK signal.

RX OK: this information is showing that the receiver is enabled. It basically means that there is valid signal with necessary strenght is received in the local end.

Device setup

The device setup screen leads you to the main monitoring options. Here the alarms can be set and main information about the Laser head.



Device Information

Device name: **FSO HEAD 1** Change
Managed head: **Pico-X (1)**

Detector alert level: **0.50 V** Change
Temperature alert level: **70 °C** Change

Auto MDI/MDI-X: **enabled** Change
NPASD: **disabled** Change

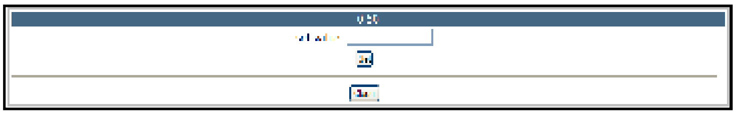
Motherboard Serial number: **000001**
Head Serial number: **0000001**

Software version: **3.2.1204 / 084C** **(factory)**
Uploaded software: **none** Update

Back to Main page

Device name: uniqe identifier of the device

Managed head: Type of the laserhead



Detector alert level: when the received level reach this value, the alarm will be triggered.

Temperature alert level: when the temperature reach this value, the alarm will be triggered.

Auto MDI/MDI-X: this enables the Auto setting for the MDI/MDI-X, some old switch types might report incompatibility here it can be switched off. (Auto MDI/MDI-X can be turned off even in the Xs systems)

NPASD (if avialable):if the reciver does not detect sufficient light power, then in the head would switch off the network connection signal. Note: During this perid the 100MB/s laser heads MGM will not be available

Motherboard Firmware version: This is the version number of the Firmware

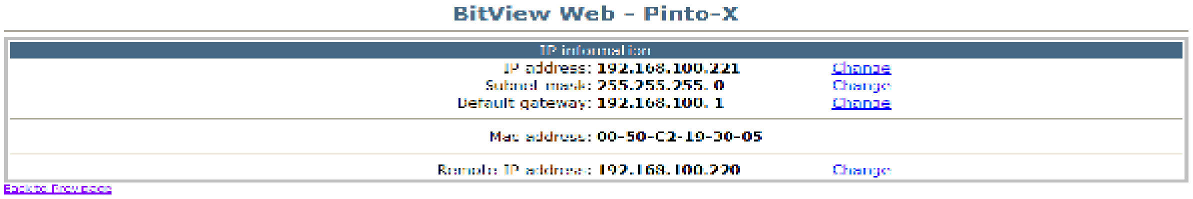
File image version: Version number of the file image

Motherboard Serial number: Mainboard serial number inside the head (Not the same as the Head Serial Number)

Head Serial number: Serial number of the unit. Should be the same number as the one on the back of the unit. If the number is missing or not match up with the one on the back, during activation this is the number you will have to let the support know.

IP Setup

Clicking on the IP Setup link you can have access to the Ethernet module of the system, this will make easy access to the IP number and/or port settings. These settings are sensitive setting and some of them cannot be restored by the user. Please always do the changes with extra care! If you have doubt in any step, do not hesitate to contact the technical support of the manufacturer website for further information.



BitView Web - Pinto-X

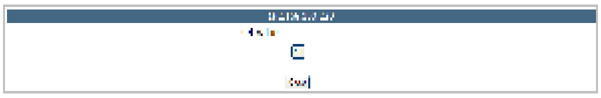
IP information

IP address: 192.168.100.221 Change
Subnet mask: 255.255.255. 0 Change
Default gateway: 192.168.100. 1 Change

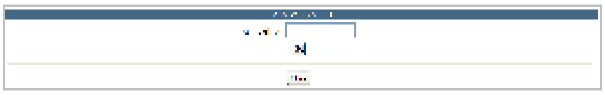
Mac address: 00-50-C2-19-30-05

Remote IP address: 192.168.100.220 Change

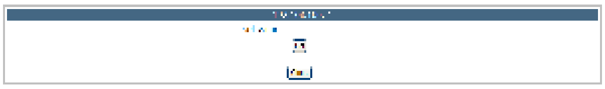
Back to Prev page



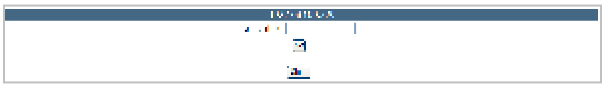
Local IP: the IP address of the local device can be set in this box. If the IP address is set retype it to your browser.
Enter only valid IP addresses, if you forget the IP address, you will have to turn to our support and in some cases return the device for reseting the IP address. Please always do the IP change with care.



Subnet mask: you can set the subnet mask of the local device.



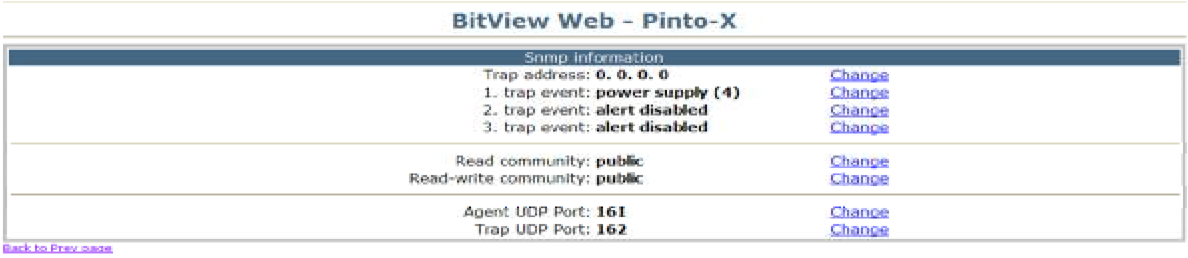
Default gateway: The default getway setting for the local device.



Remote IP:This will tell this device what the IP address of the remote device is. This setting wont change the remote units IP address, this just identify the remote device for the local device. If the IP address is not valid all diplays will go error and the display of the remote sites received level on the laserhead will be disabled!

SNMP Setup

One of the main features of the device is the SNMP(Simple Network Monitoring Protocol). The SNMP settings can be set on this page.



BitView Web - Pinto-X

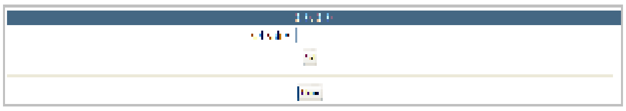
Snmp information

Trap address: **0. 0. 0. 0**	Change
1. trap event: **power supply (4)**	Change
2. trap event: **alert disabled**	Change
3. trap event: **alert disabled**	Change
Read community: **public**	Change
Read-write community: **public**	Change
Agent UDP Port: **161**	Change
Trap UDP Port: **162**	Change

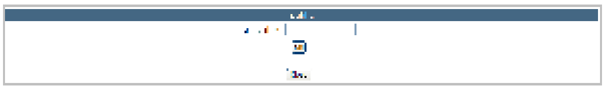
Back to Prev page

Trap address: The IP address of the SNMP trap over the network.

Trap events in the system you have possibility to setup three different trap event.
For further details on the trap event see Trap event list chapter of this book. In this section there are the settings of the SNMP Agent.



SNMP trap address: IP address of the SNMP tarp computer



Read Community and Read Write community To the setup of the Read and the Read-Write community, the preset value is public

Agent UDP Port the SNMP agent UDP port number (1…1000) the preset value is 162

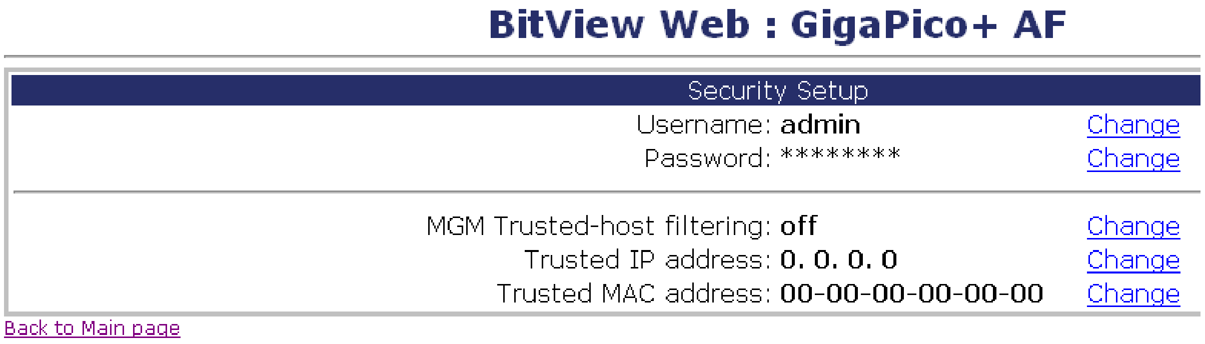
Trap UDP Port: the SNMP trap UDP port number (1…1000) the preset value is 161

Traps:
The Laserhead is sending two different traps:

LaserHeadAlarm (OID: 1.3.6.1.4.1.17857.0.1201) This trap will be sent after any of the alarms will go on (for alarm setting please see chapter 5.4)
LaserHeadAlarmCancel (OID: 1.3.6.1.4.1.17857.0.1202) After the alarm goes off this trap will be sent

Security

On the security section you can set the username and the password for the unit. If you have forget the usernam and/or the password please contact The technical support.



BitView Web : GigaPico+ AF

Security Setup

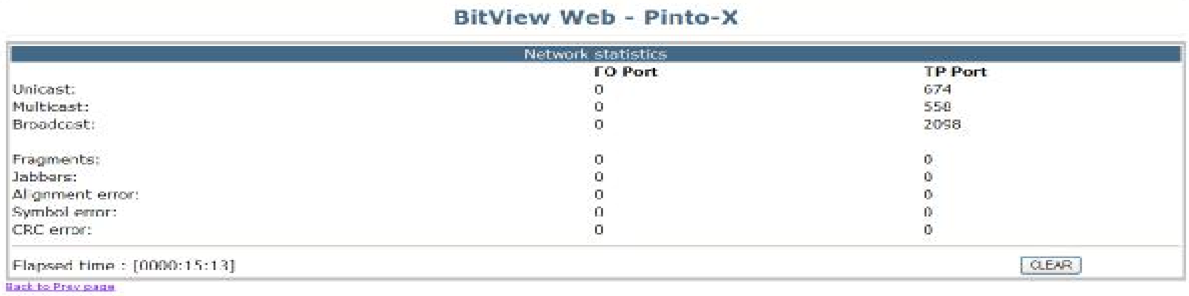
Username:	admin	Change
Password:	********	Change
MGM Trusted-host filtering:	off	Change
Trusted IP address:	0. 0. 0. 0	Change
Trusted MAC address:	00-00-00-00-00-00	Change

Back to Main page

MGM Trusted-host filtering: Here you can adjust two addresses wehre you can till in from which computer with you reach the MGM! To adjust you will hove to adjust a filter.
Filter adjust:
Off: Turned off.
IP: Only see the IP address.
MAC: Only see the MAC address
IP+MAC: Either IP or MAC address should be equal to the adjusted.
IP&MAC: Both IP and MAC addresses should be equal to the adjusted.

Network statistics page

As a new feature of the Next series of products, you can monitor the live traffic flows over the link. These figures are showing the reception on a port of FO(fibre optic from the remote end) or TP(Twisted pair, form the local connected equipment).



BitView Web - Pinto-X

Network statistics

	FO Port	TP Port
Unicast:	0	674
Multicast:	0	558
Broadcast:	0	2098
Fragments:	0	0
Jabbars:	0	0
Alignment error:	0	0
Symbol error:	0	0
CRC error:	0	0

Elapsed time : [0000:15:13]

Back to Prev page

Unicast: sending of information packets to a single destination

Multicast: is the delivery of information to a group of destinations simultaneously using the most efficient strategy to deliver the messages over each link of the network only once and only create copies when the links to the destinations split. The word "Multicast" is typically used to refer to IP Multicast, the implementation of the multicast concept on the IP routing level, where routers create optimal spanning tree distribution paths for datagram sent to a multicast destination address in real-time. But there are also other implementations of the multicast distribution strategy listed below.

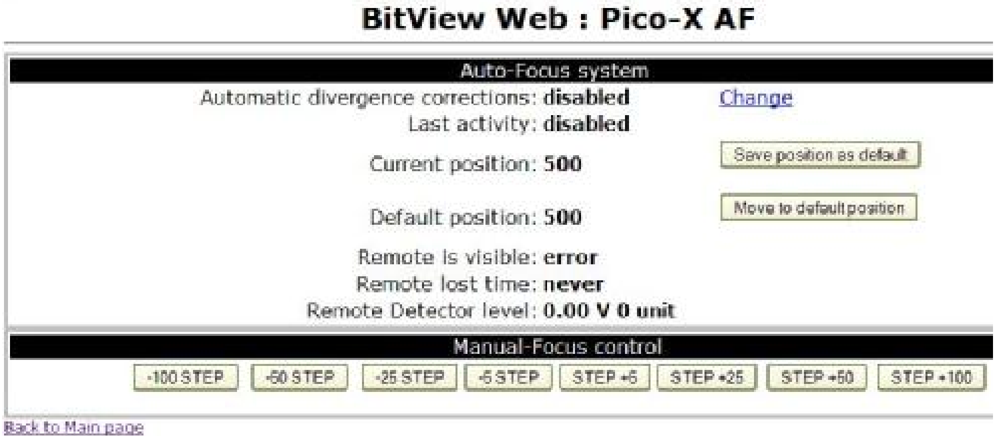
Broadcast: refers to transmitting a packet that will be received (conceptionally) by every device on the network. In practice, the scope of the broadcast is limited to a broadcast domain. Not all computer networks support broadcasting; for example, neither X.25 nor frame relay supply a broadcast capability, nor is there any form of Internet-wide broadcast. Broadcasting is largely confined to local area network (LAN) technologies, most notably Ethernet and Token Ring, where the performance impact of broadcasting is not as large as it would be in a wide area network. Both Ethernet and IPv4 use an all-ones broadcast address to indicate a broadcast packet.

Fragments: datagram can be fragmented into pieces small enough to pass over a link with a smaller MTU than the original datagram size.
Jabber: transmission of a packet on a computer network that is larger than the network's MTU. Such transmissions hog bandwidth and congest the network. Many network switches have a built-in capability to detect when a device is jabbering and block it until it resumes proper operation.
Alignment error:Decoded package alignment is faulty.
Symbol error: Coding symbol is missing or faulty.
CRC error: cyclic redundancy check is a type of hash function used to produce a checksum – a small, fixed number of bits – against a block of data, such as a packet of network traffic or a block of a computer file. The checksum is used to detect errors after transmission or storage. A CRC is computed and appended before transmission or storage, and verified afterwards by the recipient to confirm that no changes occurred on transit. CRCs are popular because they are simple to implement in binary hardware, are easy to analyze mathematically, and are particularly good at detecting common errors caused by noise in transmission channel.

Auto-focus setup (AF)

Automatic divergence corrections:

- Enabled (**auto**): adjust beam size to the best level according to the remote level.
- Disabled (**manual**): It disables the automatic adjustment routine, and lets the user adjust the beam size by using the „STEP" buttons.



BitView Web : Pico-X AF

Auto-Focus system

Automatic divergence corrections: **disabled**

Last activity: **disabled**

Current position: **500**

Default position: **500**

Remote is visible: **error**

Remote lost time: **never**

Remote Detector level: **0.00 V 0 unit**

Manual-Focus control

Last activity: which the AF (**auto focus**) has done.

- *idle*: AF was not active..
- *setting default*: saves the standard settings.
- *moving default*: return to default settings.
- *moving to open*: opens to widest beam.
- *increasing remote load*: the AF adjusts the laser beam to increase remote level.
- *decreasing remote load:* the AF adjusts the laser beam to decrease remote level.
- *optimizing remote load*: the AF adjusts the laser beam to optimal remote level.

Remote is visible: The remote side is visible or not.

Remote lost time: Shows time when remote level got lost.

Remote detector level: Shows receiving level in Volt and number of units on LCD.

Manual focus control: After setting the Manual Focus controls you can adjust the manual focus by clicking on the „STEP" buttons. You can increase the beam size, by clicking on the plus numbers or you can decrease it by clicking on the minus. The amount of the increase or the decrease depends on the number of steps .

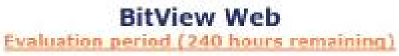
Mandatory Management Activation

Thank you for buying our product. Please read this note carefully. From software version (3.2.1218/R090x)!
The product you have bought has fully functional management software, which has limitation only in time. The unit activation request should be sent to activation@geodesy-fso.com. And the activation code will be issued, later and sent to the email address give, or can be accessed from your local distributor.

After 90 days if the system was not activated the data transmission will be degraded!

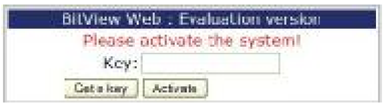
Activation process:
1. Login to the devices through a web browser using the IP:192.168.100.220,192.168.100.221
2. Default login name:admin and password:admin

3. Click on Evaluation period



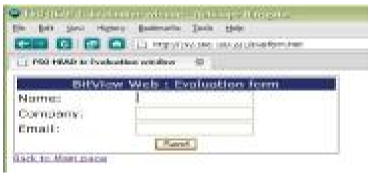
BitView Web
Evaluation period (240 hours remaining)

4. Click on Get a key



BitView Web : Evaluation version
Please activate the system!
Key:
Get a key | Activate

5. Fill in the table and click on send



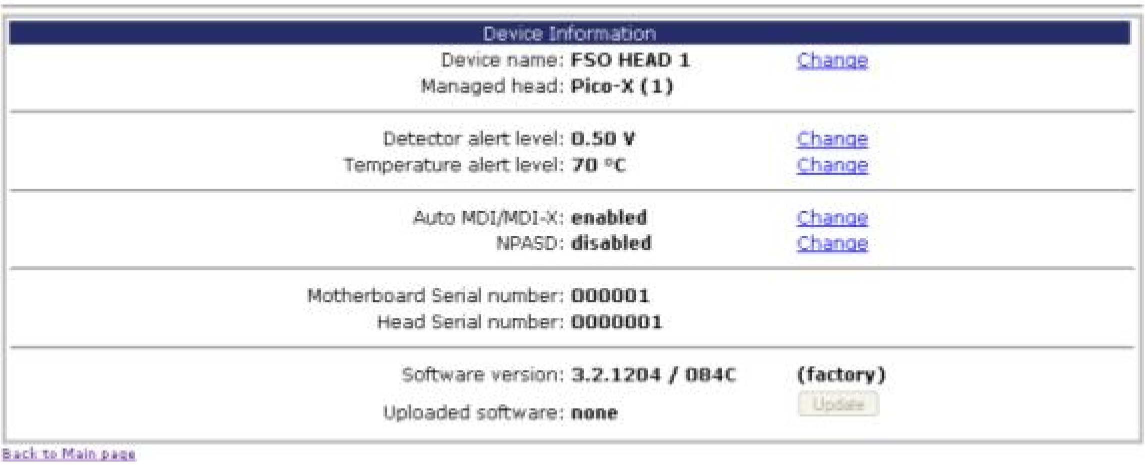
File Edit View History Bookmarks Tools Help
FSO HEAD in Evaluation window

BitView Web : Evolution form
Name:
Company:
Email:
Send
Back to Main page

6. We will return the activation key

Limitations:
- All Next-Series(100MB/s) limitation course 1-60 days unlimited, for 61-80 days 10MB/s, for 81-90 days 1MB/s, beyond 90 days 100KB/s (MGM-Option).
- All GigaNext-Series(1000 MB/s) will be limited after the 90th day, when the whole bandwidth will be blocked, except the management system.

7.2 Firmware update



Device Information

Device name: **FSO HEAD 1** Change
Managed head: **Pico-X (1)**

Detector alert level: **0.50 V** Change
Temperature alert level: **70 °C** Change

Auto MDI/MDI-X: **enabled** Change
NPASD: **disabled** Change

Motherboard Serial number: **000001**
Head Serial number: **0000001**

Software version: **3.2.1204 / 084C** **(factory)**
Uploaded software: **none** Update

Back to Main page

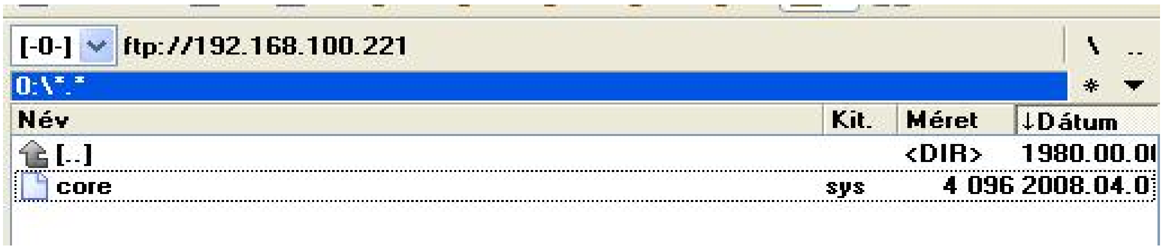
The firmware update has the following steps:

Run FTP client
Log-in to the Laser-head
Copy Geodesy_FWUpdate_Vxx.xbn over
Log in the laserhead
Click on update
Wait 50-60 seconds
Restart the laserhead

Run FTP client
FTP client setup
IP address: the IP address of the device (192.168.100.220 or 192.168.100.221 as a factory default) or the IP address you gave to the system earlier – same as the IP address for the Web management.

User name: same as for the web management (default admin)
Password: same as for the web management (default admin)

If you have passive mode please turn it off, otherwise the system will not connect.

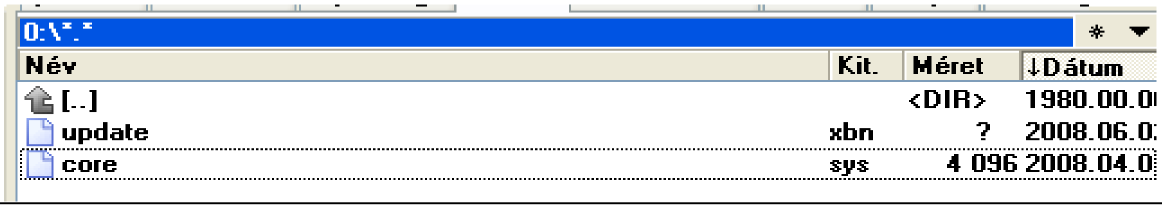


[-0-] ftp://192.168.100.221

0:*.*

Név	Kit.	Méret	↓Dátum
[..]		<DIR>	1980.00.0
core	sys	4 096	2008.04.0

copy the .xbn file over to the Laserhead

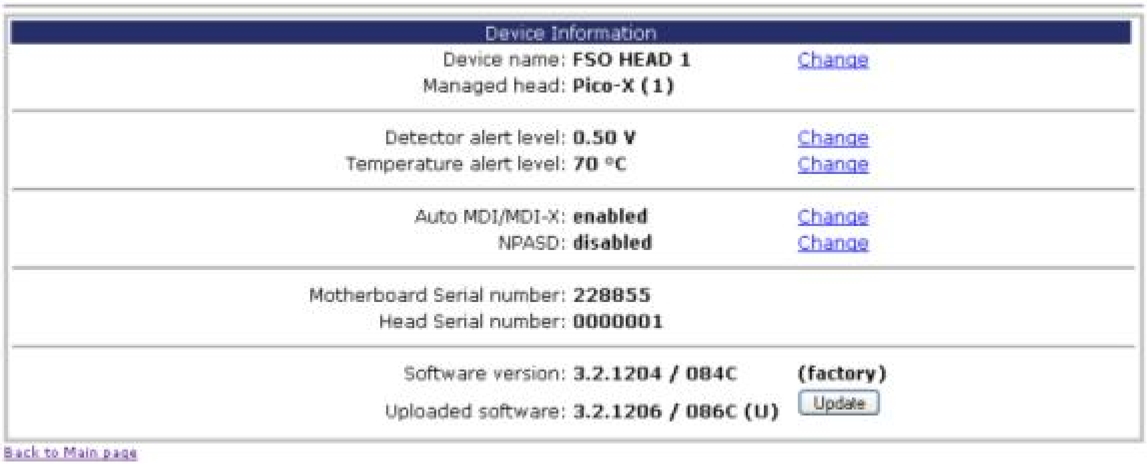


0:*.*

Név	Kit.	Méret	↓Dátum
[..]		<DIR>	1980.00.0
update	xbn	?	2008.06.0
core	sys	4 096	2008.04.0

Log off the FTP server

Now the Update button will be active



Device Information		
Device name:	**FSO HEAD 1**	Change
Managed head:	**Pico-X (1)**	
Detector alert level:	**0.50 V**	Change
Temperature alert level:	**70 °C**	Change
Auto MDI/MDI-X:	**enabled**	Change
NPASD:	**disabled**	Change
Motherboard Serial number:	**228855**	
Head Serial number:	**0000001**	
Software version:	**3.2.1204 / 084C**	**(factory)**
Uploaded software:	**3.2.1206 / 086C (U)**	Update

Back to Main page

Click on update and the update process will start it takes upto 60 seconds. The LEDs on the back of the device will go off than lit one after the other.

Make sure that the system power is fixed and the power will not go off during the update process. If the LEDs froze, wait 2-3 minutes before unplugging the power cable, and repluging again.

7.3 Reloading factory default settings

Should you need to reload the original factory settings follow the steps below.

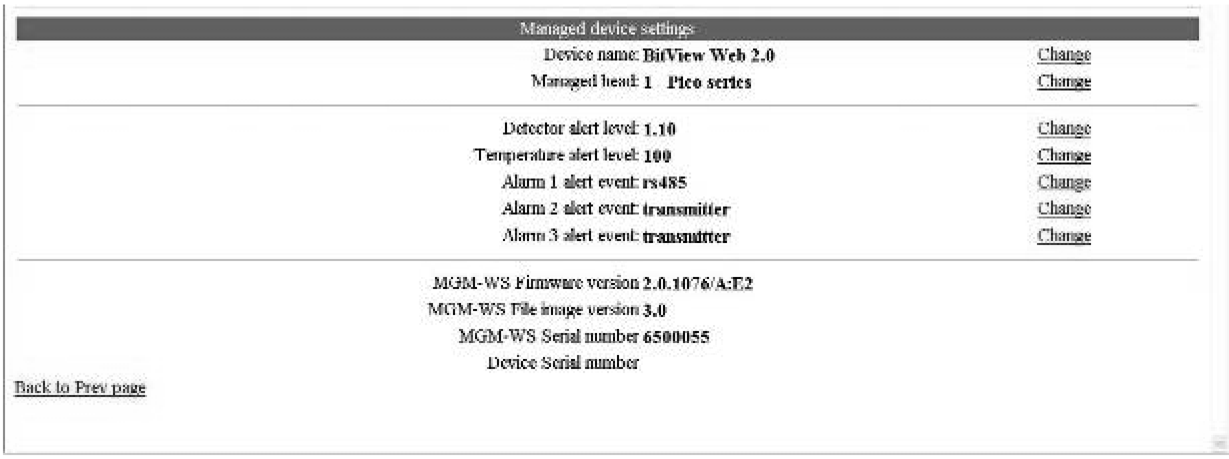
1. unplug the POE RJ45 cable
2. replug the POE RJ45 cable
3. unplug the POE RJ45 cable within 3 seconds
4. repeat procedure 3 times.
5. plug the POE RJ45 cable into the system, and leave it plugged in.

After this the system resets the following information to the factory default.

- IP address
- Username
- Password
- Device name
- SNMP settings
- Alerts
- Auto MDI/MDIX
- NPASD (if avialable):if the reciver does not detect sufficient light power, then in the head would switch off the network connection signal. Note: During this perid the 100MB/s laser heads MGM will not be available.

7.4 Setting up the SNMP

Please check the GD view manual for details how to proceed to this point



Managed device settings

Device name: BitView Web 2.0 Change
Managed head: 1 Pico series Change

Detector alert level: 1.10 Change
Temperature alert level: 100 Change
Alarm 1 alert event: rs485 Change
Alarm 2 alert event: transmitter Change
Alarm 3 alert event: transmitter Change

MGM-WS Firmware version 2.0.1076/A:E2
MGM-WS File image version 3.0
MGM-WS Serial number 6500055
Device Serial number

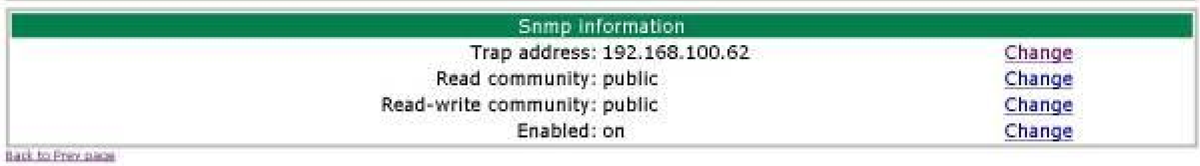
Back to Prev page

1. Figure

On Figure 1 you can see our test setting. The GD-View is sending 3 traps
LaserHeadAlarm (OID: 1.3.6.1.4.1.17857.0.1201) This trap will be sent after any of the alarms will go on (for alarm setting please see chapter 5.4)
LaserHeadAlarmCancel (OID: 1.3.6.1.4.1.17857.0.1202) After the alarm goes off this trap will be sent
DeviceDown (OID: 1.3.6.1.4.1.17857.0.1103) This trap is being sent when the SNMP agent is disabled

Even if you have one laerhead attached to one GD-View, or you are on the live network you can generate traps without, causing any problems, with the testing.

For these testing purposes please set Alarm1 to RS485(this will generate traps), and Alarm2 Alarm3 to transmitter(this wont generate traps, so wont disturb the testing)



Snmp information	
Trap address: 192.168.100.62	Change
Read community: public	Change
Read-write community: public	Change
Enabled: on	Change

Back to Prev page

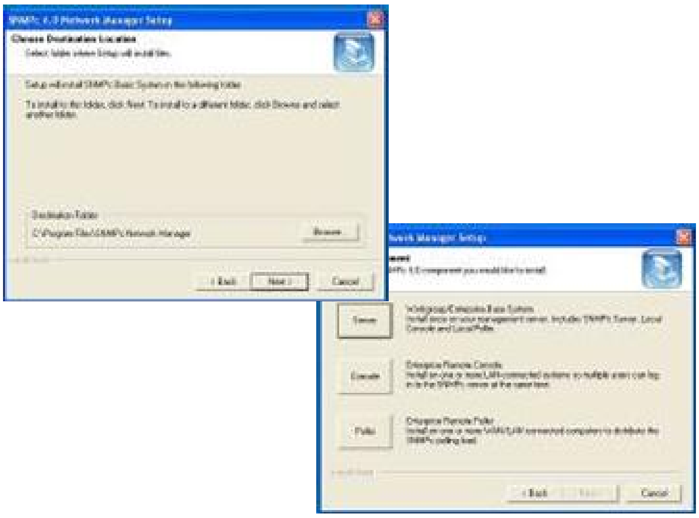
2. Figure

On figure 2 the settings can be seen.
Change the Trap address to the MGM console IP address which will have the SMNPc installed
Enabled must be set to on the function will disable the SNMP agent.

After this was set the GD view is ready to send out the Trap messages, to the Trap Addressed PC

7.4.1 SNMPc Installation

First run snmpc600eval.exe file from the CD.



SNMPc 6.0 Network Manager Setup

Choose Destination Location

Select folder where Setup will install files.

Setup will install SNMPc Basic System in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\Program Files\SNMPc Network Manager

...twork Manager Setup

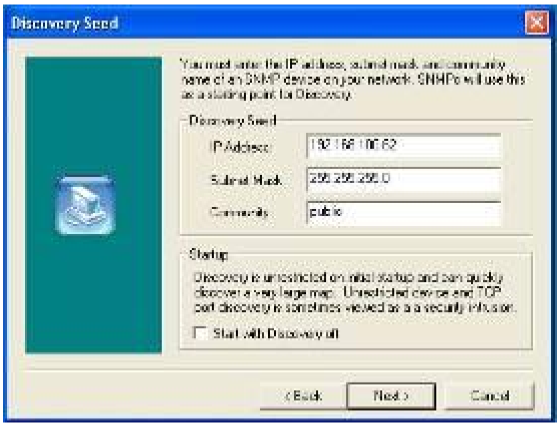
...Pc 6.0 component you would like to install

Workgroup/Enterprise Base System
Install once on your management server. Includes SNMPc Server, Local Console and Local Poller.

Enterprise Remote Console
Install on one or more LAN-connected systems so multiple users can log in to the SNMPc server at the same time.

Enterprise Remote Poller
Install on one or more WAN/LAN connected computers to distribute the SNMPc polling load.

Run through the setup process by clicking next



Discovery Seed

You must enter the IP address, subnet mask and community name of an SNMP device on your network. SNMPc will use this as a starting point for Discovery.

Discovery Seed

IP Address: 192.168.100.62

Subnet Mask: 255.255.255.0

Community: public

Startup

Discovery is unrestricted on initial startup and can quickly discover a very large map. Unrestricted device and TCP port discovery is sometimes viewed as a a security intrusion.

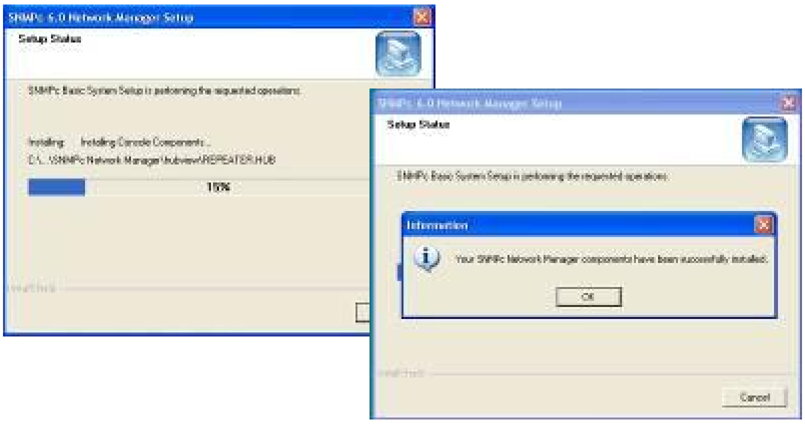
□ Start with Discovery off

When the setup asks for the discovery seed enter you own IP address, Subnet mask a community

After the setup was finished hit OK. Your PC might ask for a restart, in that cases please restart your PC

SNMPC

7.4.2 Configuration of the SNMPc Management console



SNMPc 6.0 Network Manager Setup

Setup Status

SNMPc Basic System Setup is performing the requested operations.

Installing: Installing Console Components...

C:\...\SNMPc Network Manager\hubview\REPEATER.HUB

15%

SNMPc 6.0 Network Manager Setup

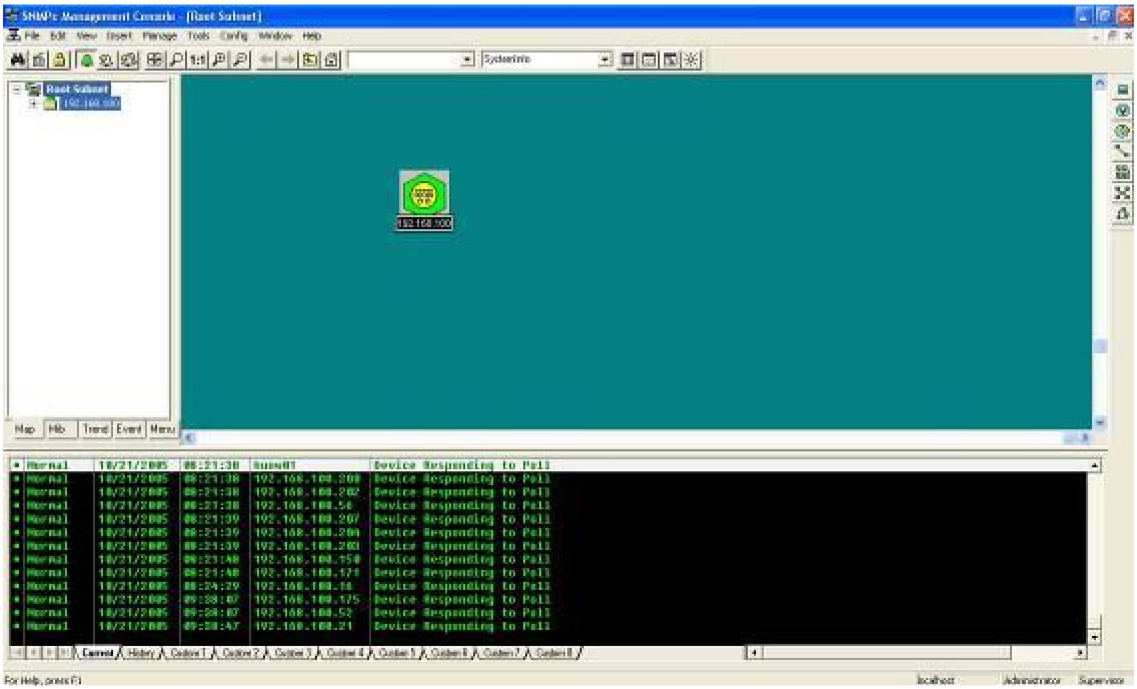
Setup Status

SNMPc Basic System Setup is performing the requested operations.

Information

Your SNMPc Network Manager components have been successfully installed.

Click on Start => Programs => SNMPc network manager => Startup system. This will start the SNMPc Management console. Can be seen on Figure 3

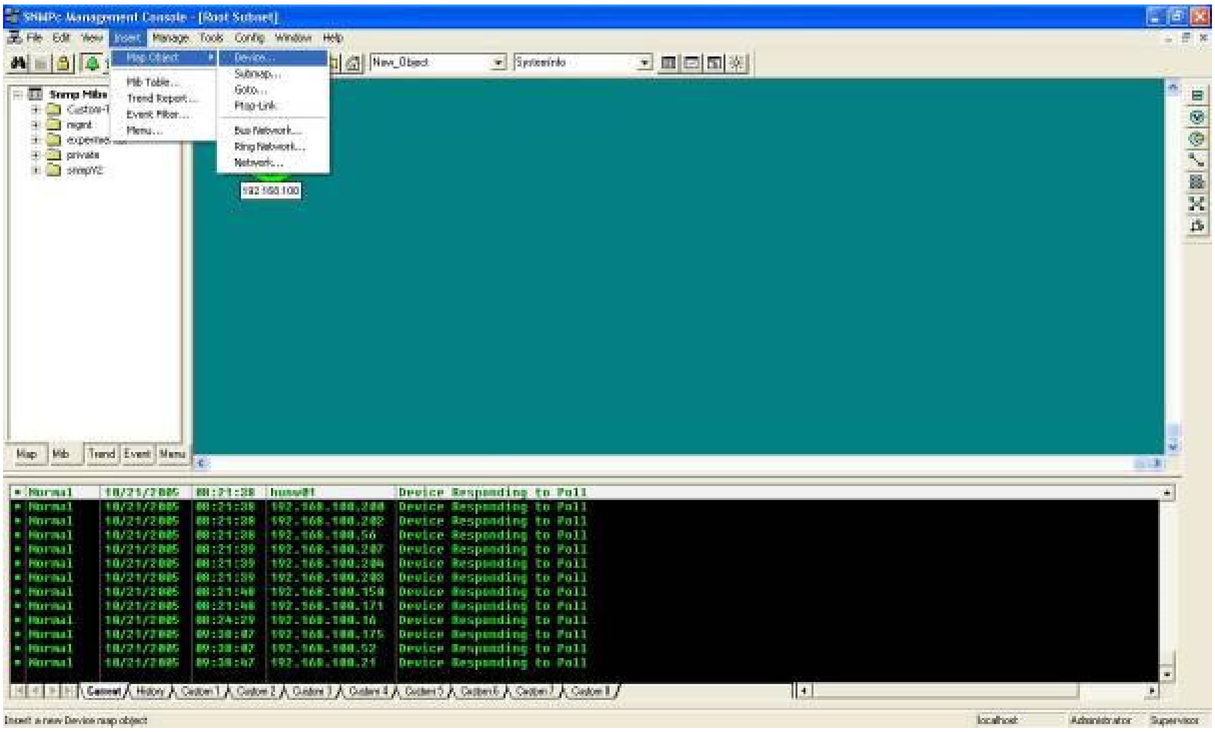

SNMPc Management Console - [Root Subnet]
File Edit View Insert Manage Tools Config Window Help
SystemInfo
Root Subnet
192.168.100
192.168.100
Map Mib Trend Event Menu
Current History Custom 1 Custom 2 Custom 3 Custom 4 Custom 5 Custom 6 Custom 7 Custom 8
localhost Administrator Supervisor

```
Normal  10/21/2005  08:21:38  huawe01          Device Responding to Poll
Normal  10/21/2005  08:21:38  192.168.100.200  Device Responding to Poll
Normal  10/21/2005  08:21:38  192.168.100.202  Device Responding to Poll
Normal  10/21/2005  08:21:38  192.168.100.56   Device Responding to Poll
Normal  10/21/2005  08:21:39  192.168.100.207  Device Responding to Poll
Normal  10/21/2005  08:21:39  192.168.100.204  Device Responding to Poll
Normal  10/21/2005  08:21:39  192.168.100.203  Device Responding to Poll
Normal  10/21/2005  08:21:40  192.168.100.150  Device Responding to Poll
Normal  10/21/2005  08:21:40  192.168.100.171  Device Responding to Poll
Normal  10/21/2005  08:24:29  192.168.100.16   Device Responding to Poll
Normal  10/21/2005  09:38:07  192.168.100.175  Device Responding to Poll
Normal  10/21/2005  09:38:07  192.168.100.52   Device Responding to Poll
Normal  10/21/2005  09:38:47  192.168.100.21   Device Responding to Poll
```

For Help, press F1

3. Figure

To add the GD-View to the console click on Insert => Map Object => Device. As it is shown on Figure 4

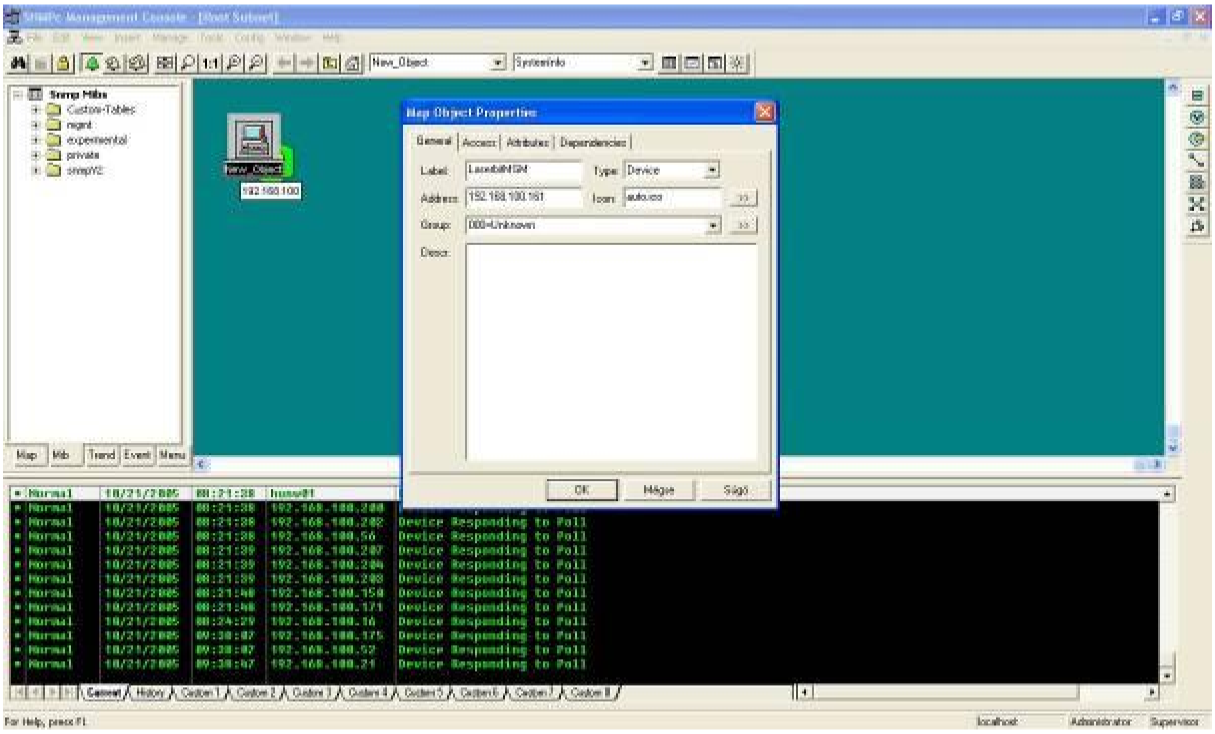


```
Normal  10/21/2005  08:21:38  huawe01          Device Responding to Poll
Normal  10/21/2005  08:21:38  192.168.100.200  Device Responding to Poll
Normal  10/21/2005  08:21:38  192.168.100.202  Device Responding to Poll
Normal  10/21/2005  08:21:38  192.168.100.56   Device Responding to Poll
Normal  10/21/2005  08:21:39  192.168.100.207  Device Responding to Poll
Normal  10/21/2005  08:21:39  192.168.100.204  Device Responding to Poll
Normal  10/21/2005  08:21:39  192.168.100.203  Device Responding to Poll
Normal  10/21/2005  08:21:40  192.168.100.150  Device Responding to Poll
Normal  10/21/2005  08:21:40  192.168.100.171  Device Responding to Poll
Normal  10/21/2005  08:24:29  192.168.100.16   Device Responding to Poll
Normal  10/21/2005  09:38:07  192.168.100.175  Device Responding to Poll
Normal  10/21/2005  09:38:07  192.168.100.52   Device Responding to Poll
Normal  10/21/2005  09:38:47  192.168.100.21   Device Responding to Poll
```

Insert a new Device map object

4. Figure

After the Map Onject was added, the properties should be set:
Label : GeoDesy-FSO MGM (cannot contain spaces, or special caracters) see Figure



Map Object Properties

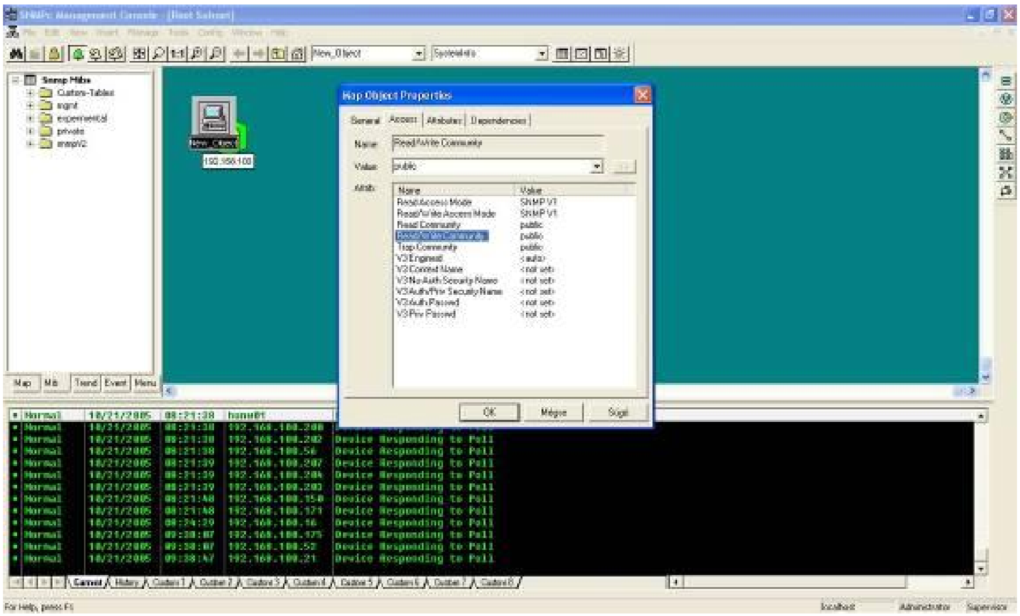
General | Access | Attributes | Dependencies

Label: LacebiMGM Type: Device
Address: 192.168.100.161 Icon: auto.ico
Group: 000=Unknown
Descr:

```
Normal  10/21/2005  08:21:38  hunu01
Normal  10/21/2005  08:21:38  192.168.100.200
Normal  10/21/2005  08:21:38  192.168.100.202  Device Responding to Poll
Normal  10/21/2005  08:21:38  192.168.100.56   Device Responding to Poll
Normal  10/21/2005  08:21:39  192.168.100.207  Device Responding to Poll
Normal  10/21/2005  08:21:39  192.168.100.204  Device Responding to Poll
Normal  10/21/2005  08:21:39  192.168.100.203  Device Responding to Poll
Normal  10/21/2005  08:21:40  192.168.100.150  Device Responding to Poll
Normal  10/21/2005  08:21:40  192.168.100.171  Device Responding to Poll
Normal  10/21/2005  08:24:29  192.168.100.16   Device Responding to Poll
Normal  10/21/2005  09:38:07  192.168.100.175  Device Responding to Poll
Normal  10/21/2005  09:38:07  192.168.100.52   Device Responding to Poll
Normal  10/21/2005  09:38:47  192.168.100.21   Device Responding to Poll
```

SNMPc Management Console - [Root Subnet]
File Edit View Insert Manage Tools Config Window Help
New_Object
SystemInfo
Snmp Mibs
Custom-Tables
mgmt
experimental
private
snmpV2
New_Object
192.168.100.100
Map Mib Trend Event Menu
OK Mégse Súgó
Current History Custom 1 Custom 2 Custom 3 Custom 4 Custom 5 Custom 6 Custom 7 Custom 8
For Help, press F1
localhost Administrator Supervisor

On the Access Tab
Read Access Mode: SNMPV1
Read/Write Access Mode: SNMPV1
Read community: public
Read/Write Community: public
Trap community: public
The rest of the setting can be left on factory default.



Map Object Properties

General | Access | Attributes | Dependencies

Name: Read/Write Community
Value: public

Attrib:

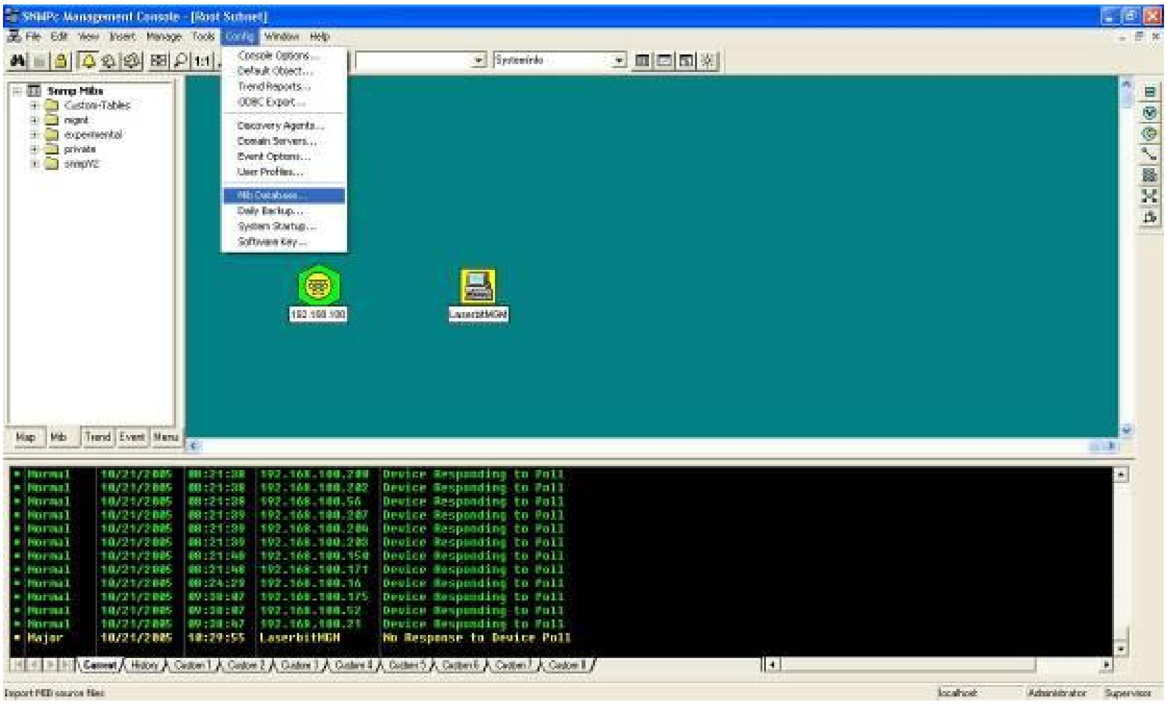
Name	Value
Read Access Mode	SNMP V1
Read/Write Access Mode	SNMP V1
Read Community	public
Read/Write Community	public
Trap Community	public
V3 EngineId	<auto>
V3 Context Name	<not set>
V3 No Auth Security Name	<not set>
V3 Auth/Priv Security Name	<not set>
V3 Auth Passwd	<not set>
V3 Priv Passwd	<not set>

```
Normal  10/21/2005  08:21:38  hunu01
Normal  10/21/2005  08:21:38  192.168.100.200
Normal  10/21/2005  08:21:38  192.168.100.202  Device Responding to Poll
Normal  10/21/2005  08:21:38  192.168.100.56   Device Responding to Poll
Normal  10/21/2005  08:21:39  192.168.100.207  Device Responding to Poll
Normal  10/21/2005  08:21:39  192.168.100.204  Device Responding to Poll
Normal  10/21/2005  08:21:39  192.168.100.203  Device Responding to Poll
Normal  10/21/2005  08:21:40  192.168.100.150  Device Responding to Poll
Normal  10/21/2005  08:21:40  192.168.100.171  Device Responding to Poll
Normal  10/21/2005  08:24:29  192.168.100.16   Device Responding to Poll
Normal  10/21/2005  09:38:07  192.168.100.175  Device Responding to Poll
Normal  10/21/2005  09:38:07  192.168.100.52   Device Responding to Poll
Normal  10/21/2005  09:38:47  192.168.100.21   Device Responding to Poll
```

SNMPc Management Console - [Root Subnet]
New_Object
SystemInfo
Snmp Mibs
Custom-Tables
mgmt
experimental
private
snmpV2
New_Object
192.168.100.100
Map Mib Trend Event Menu
OK Mégse Súgó
Current History Custom 1 Custom 2 Custom 3 Custom 4 Custom 5 Custom 6 Custom 7 Custom 8
For Help, press F1
localhost Administrator Supervisor

7.4.3 Compiling GeoDesy-FSO Mib file

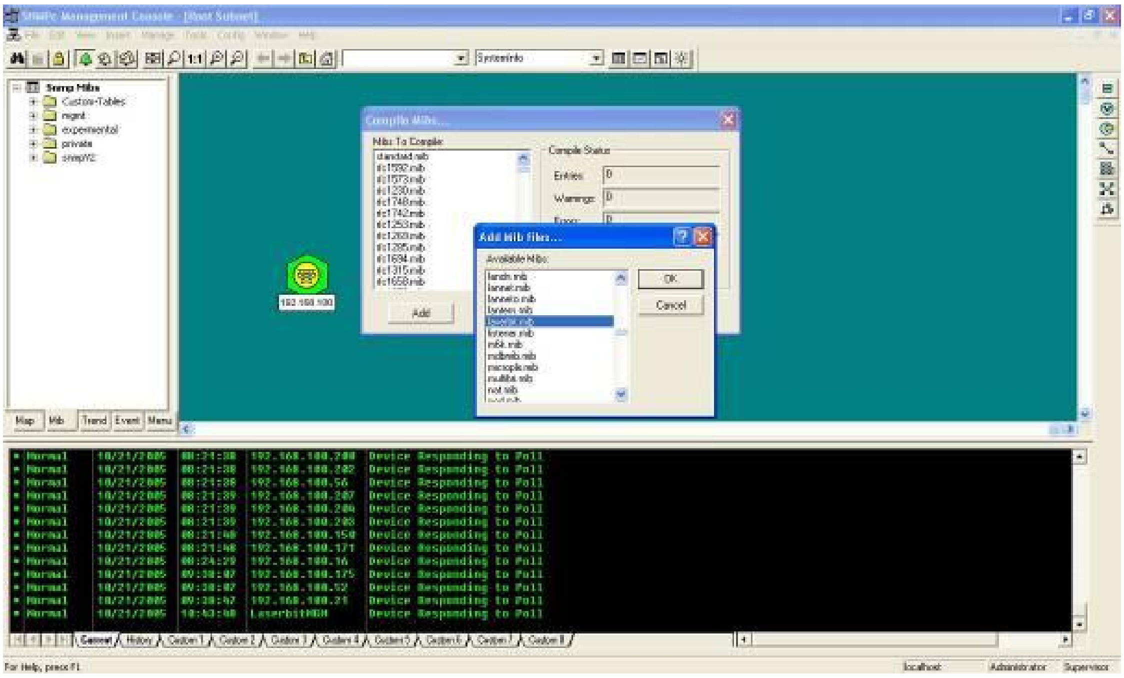
First copy the Mib file (GeoDesy-FSO.mib [Source: CD:\Mib\V07\GeoDesy-FSO.mib]). Copy this file over to : C:\Program Files\SNMPc Network Manager\mibfiles\
To Compile the MIB file to the SNMPc Click on Config=>Mib Database



```
• Normal  10/21/2005  08:21:38  192.168.100.200  Device Responding to Poll
• Normal  10/21/2005  08:21:38  192.168.100.202  Device Responding to Poll
• Normal  10/21/2005  08:21:38  192.168.100.56   Device Responding to Poll
• Normal  10/21/2005  08:21:39  192.168.100.207  Device Responding to Poll
• Normal  10/21/2005  08:21:39  192.168.100.204  Device Responding to Poll
• Normal  10/21/2005  08:21:39  192.168.100.203  Device Responding to Poll
• Normal  10/21/2005  08:21:40  192.168.100.150  Device Responding to Poll
• Normal  10/21/2005  08:21:40  192.168.100.171  Device Responding to Poll
• Normal  10/21/2005  08:24:29  192.168.100.16   Device Responding to Poll
• Normal  10/21/2005  09:38:07  192.168.100.175  Device Responding to Poll
• Normal  10/21/2005  09:38:07  192.168.100.52   Device Responding to Poll
• Normal  10/21/2005  09:38:47  192.168.100.21   Device Responding to Poll
• Major   10/21/2005  10:29:55  LaserbitMGH      No Response to Device Poll
```

Import MIB source files

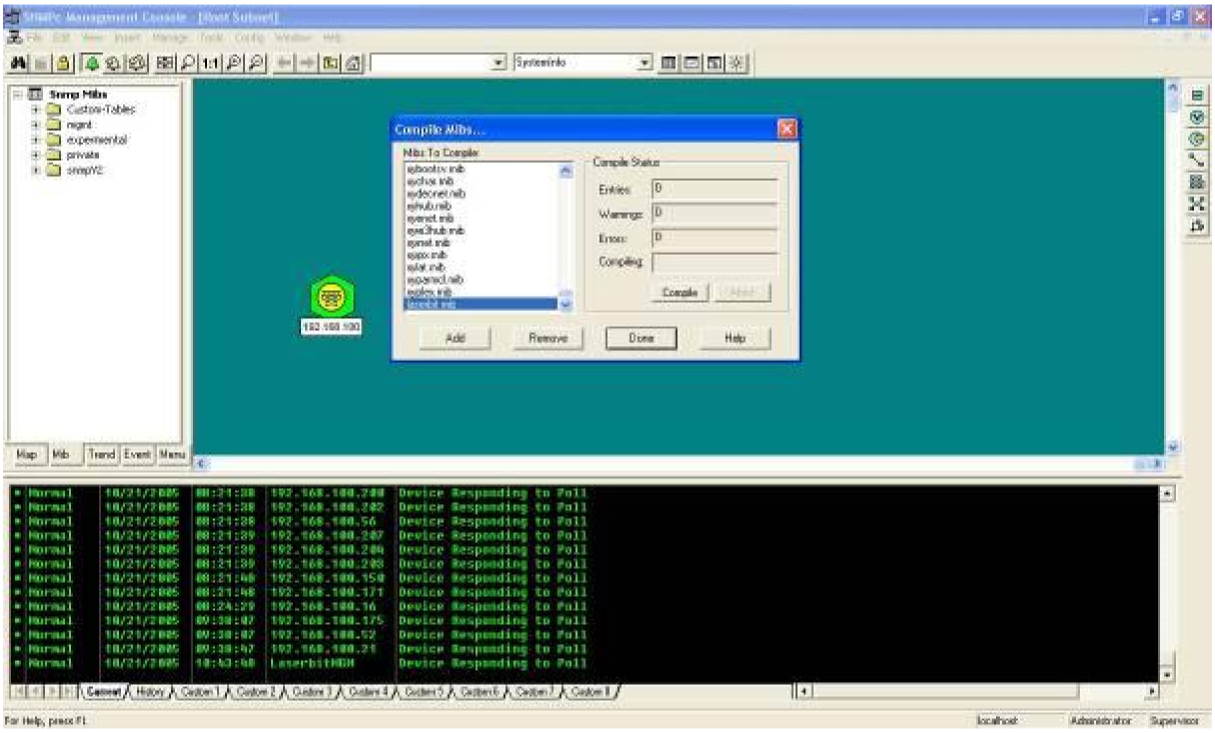
After opening the Mib Database, you should add the MIB file to the Database: Click on Add. Add Mib files: find GeoDesy-FSO.mib, then click OK



```
• Normal  10/21/2005  08:21:38  192.168.100.200  Device Responding to Poll
• Normal  10/21/2005  08:21:38  192.168.100.202  Device Responding to Poll
• Normal  10/21/2005  08:21:38  192.168.100.56   Device Responding to Poll
• Normal  10/21/2005  08:21:39  192.168.100.207  Device Responding to Poll
• Normal  10/21/2005  08:21:39  192.168.100.204  Device Responding to Poll
• Normal  10/21/2005  08:21:39  192.168.100.203  Device Responding to Poll
• Normal  10/21/2005  08:21:40  192.168.100.150  Device Responding to Poll
• Normal  10/21/2005  08:21:40  192.168.100.171  Device Responding to Poll
• Normal  10/21/2005  08:24:29  192.168.100.16   Device Responding to Poll
• Normal  10/21/2005  09:38:07  192.168.100.175  Device Responding to Poll
• Normal  10/21/2005  09:38:07  192.168.100.52   Device Responding to Poll
• Normal  10/21/2005  09:38:47  192.168.100.21   Device Responding to Poll
• Normal  10/21/2005  10:43:48  LaserbitMGH      Device Responding to Poll
```

For Help, press F1

After you hit OK you have added the Mib file to the database now you will have to compile it to the management console. So find again GeoDesy-FSO.mib and highlight it. Than Hit compile. It will ask you whether you want to compile it click on Yes.

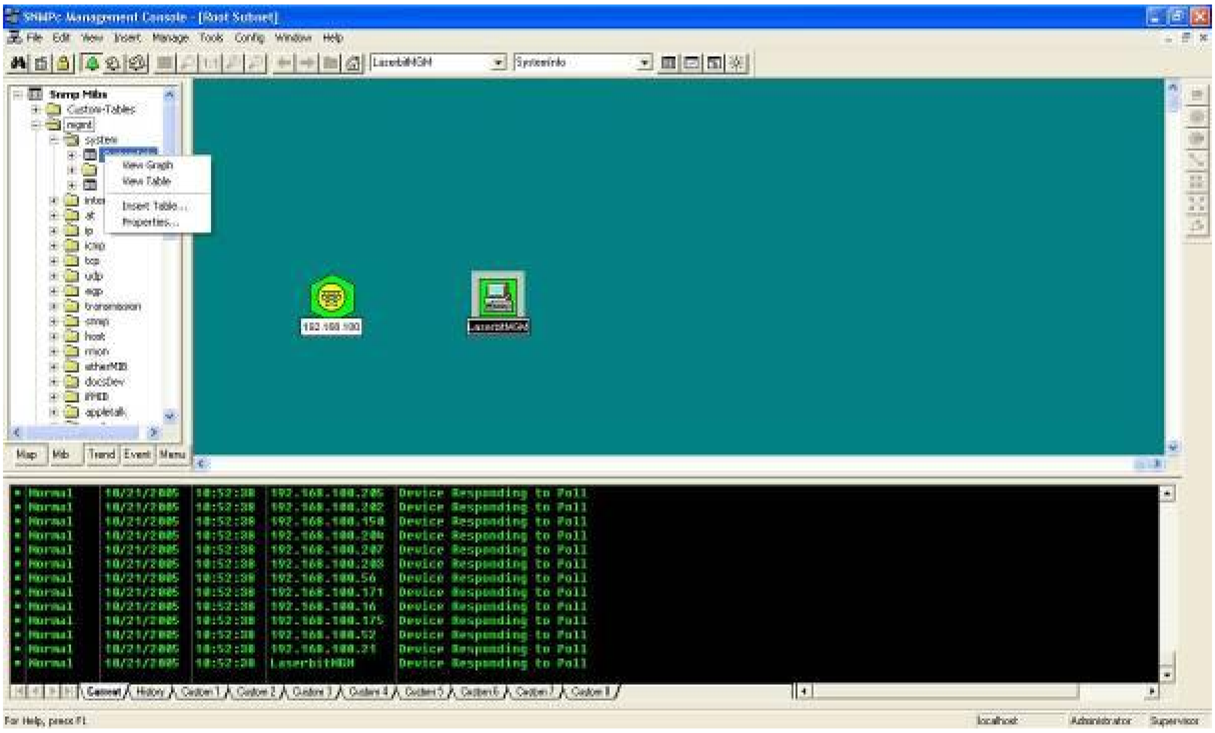


Entries: 0
Warnings: 0
Errors: 0
Compiling:

```
• Normal   10/21/2005  08:21:38  192.168.100.200  Device Responding to Poll
• Normal   10/21/2005  08:21:38  192.168.100.202  Device Responding to Poll
• Normal   10/21/2005  08:21:38  192.168.100.56   Device Responding to Poll
• Normal   10/21/2005  08:21:39  192.168.100.207  Device Responding to Poll
• Normal   10/21/2005  08:21:39  192.168.100.204  Device Responding to Poll
• Normal   10/21/2005  08:21:39  192.168.100.203  Device Responding to Poll
• Normal   10/21/2005  08:21:40  192.168.100.150  Device Responding to Poll
• Normal   10/21/2005  08:21:40  192.168.100.171  Device Responding to Poll
• Normal   10/21/2005  08:24:29  192.168.100.16   Device Responding to Poll
• Normal   10/21/2005  09:38:47  192.168.100.175  Device Responding to Poll
• Normal   10/21/2005  09:38:47  192.168.100.52   Device Responding to Poll
• Normal   10/21/2005  09:38:47  192.168.100.21   Device Responding to Poll
• Normal   10/21/2005  10:43:48  LaserbitMGH      Device Responding to Poll
```

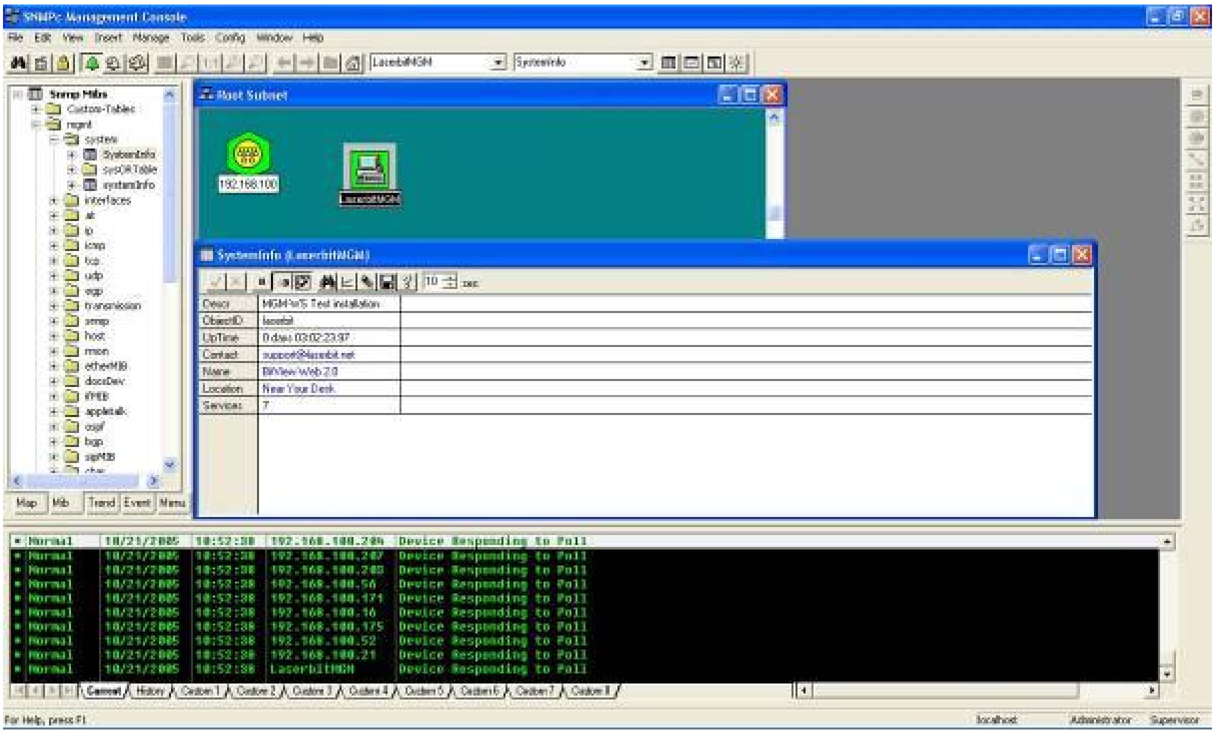
7.4.4 Using SNMP to monitor the link

First click on the GeoDesy-FSO Object to highlight it.
Open mgmt/system/SystemInfo right click on the object and view Table



```
• Normal   10/21/2005   10:52:38   192.168.100.205   Device Responding to Poll
• Normal   10/21/2005   10:52:38   192.168.100.202   Device Responding to Poll
• Normal   10/21/2005   10:52:38   192.168.100.150   Device Responding to Poll
• Normal   10/21/2005   10:52:38   192.168.100.204   Device Responding to Poll
• Normal   10/21/2005   10:52:38   192.168.100.207   Device Responding to Poll
• Normal   10/21/2005   10:52:38   192.168.100.203   Device Responding to Poll
• Normal   10/21/2005   10:52:38   192.168.100.56    Device Responding to Poll
• Normal   10/21/2005   10:52:38   192.168.100.171   Device Responding to Poll
• Normal   10/21/2005   10:52:38   192.168.100.16    Device Responding to Poll
• Normal   10/21/2005   10:52:38   192.168.100.175   Device Responding to Poll
• Normal   10/21/2005   10:52:38   192.168.100.52    Device Responding to Poll
• Normal   10/21/2005   10:52:38   192.168.100.21    Device Responding to Poll
• Normal   10/21/2005   10:52:38   LaserbitMGM       Device Responding to Poll
```

This table will show you the main System information Table:

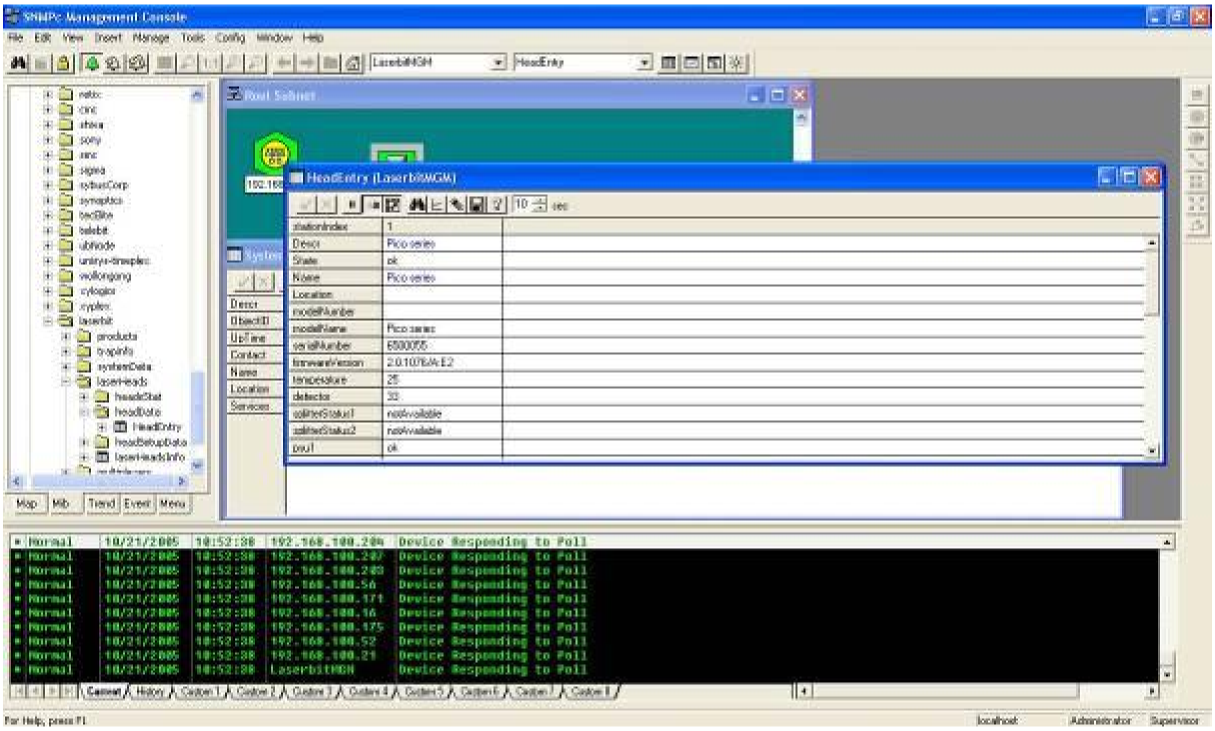


Descr	MGM-WS Test installation
ObjectID	laserbit
UpTime	0 days 03:02:23.37
Contact	support@laserbit.net
Name	BitView Web 2.0
Location	Near Your Desk
Services	7

```
• Normal   10/21/2005   10:52:38   192.168.100.204   Device Responding to Poll
• Normal   10/21/2005   10:52:38   192.168.100.207   Device Responding to Poll
• Normal   10/21/2005   10:52:38   192.168.100.203   Device Responding to Poll
• Normal   10/21/2005   10:52:38   192.168.100.56    Device Responding to Poll
• Normal   10/21/2005   10:52:38   192.168.100.171   Device Responding to Poll
• Normal   10/21/2005   10:52:38   192.168.100.16    Device Responding to Poll
• Normal   10/21/2005   10:52:38   192.168.100.175   Device Responding to Poll
• Normal   10/21/2005   10:52:38   192.168.100.52    Device Responding to Poll
• Normal   10/21/2005   10:52:38   192.168.100.21    Device Responding to Poll
• Normal   10/21/2005   10:52:38   LaserbitMGM       Device Responding to Poll
```

To see the head entries open: private/GeoDesy-FSO/headData

Right click on the head entry table and view table.


SNMPc Management Console
File Edit View Insert Manage Tools Config Window Help
LaserbitMGM
HeadEntry
Root Subnet
HeadEntry (LaserbitMGM)
10 sec
Map Mib Trend Event Menu
Current History Custom 1 Custom 2 Custom 3 Custom 4 Custom 5 Custom 6 Custom 7 Custom 8
For Help, press F1
localhost Administrator Supervisor

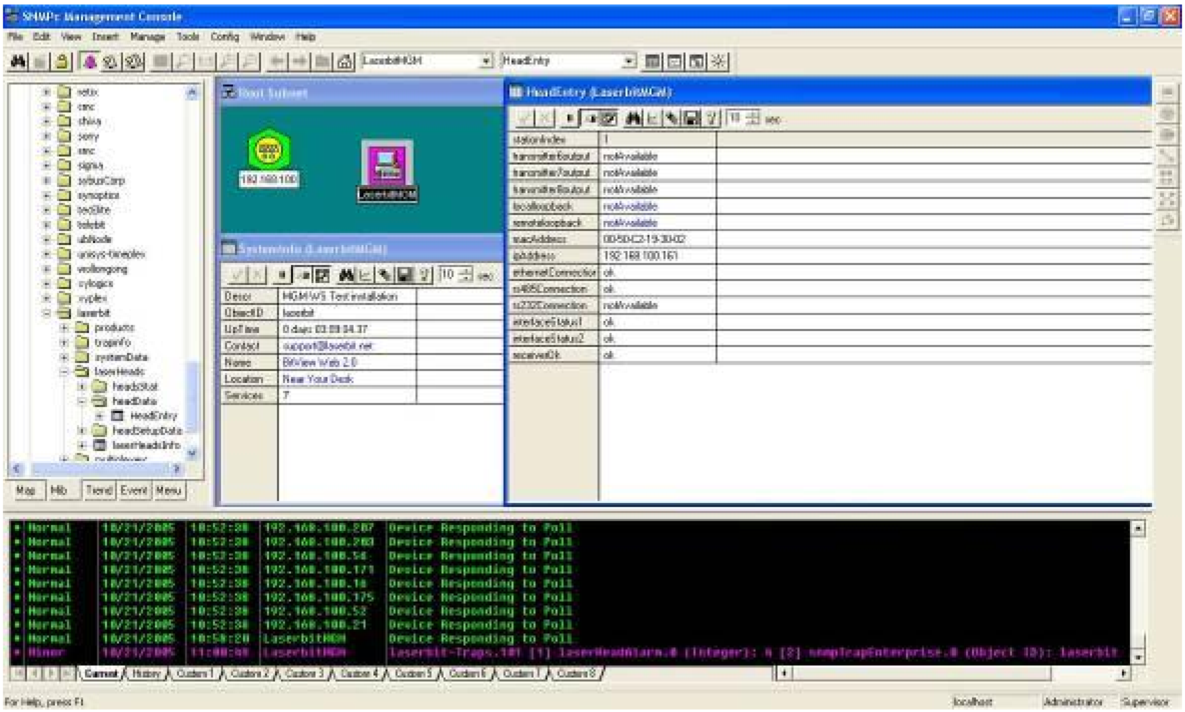
stationIndex	1
Descr	Pico series
State	ok
Name	Pico series
Location	
modelNumber	
modelName	Pico series
serialNumber	6500055
firmwareVersion	2.0.1076AcE2
temperature	25
detector	33
splitterStatus1	notAvailable
splitterStatus2	notAvailable
psu1	ok

```
Normal  10/21/2005  10:52:38  192.168.100.204  Device Responding to Poll
Normal  10/21/2005  10:52:38  192.168.100.207  Device Responding to Poll
Normal  10/21/2005  10:52:38  192.168.100.200  Device Responding to Poll
Normal  10/21/2005  10:52:38  192.168.100.56   Device Responding to Poll
Normal  10/21/2005  10:52:38  192.168.100.171  Device Responding to Poll
Normal  10/21/2005  10:52:38  192.168.100.16   Device Responding to Poll
Normal  10/21/2005  10:52:38  192.168.100.175  Device Responding to Poll
Normal  10/21/2005  10:52:38  192.168.100.52   Device Responding to Poll
Normal  10/21/2005  10:52:38  192.168.100.21   Device Responding to Poll
Normal  10/21/2005  10:52:38  LaserbitMGM      Device Responding to Poll
```

Now the SNMP is completely set up.

7.4.5 Generating failure

While the SNMP is working, if you would like to see that actually, it really does what it suppose to be, unplug the RJ11 (RS485) cable from the GD-View.


SNMPc Management Console
File Edit View Insert Manage Tools Config Window Help
LaserbitHGM
HeadEntry
Root Subnet
192.168.100
LaserbitHGM
Map Mib Trend Event Menu
Current History Custom 1 Custom 2 Custom 3 Custom 4 Custom 5 Custom 6 Custom 7 Custom 8
For Help, press F1
localhost Administrator Supervisor

SystemInfo (LaserbitHGM)

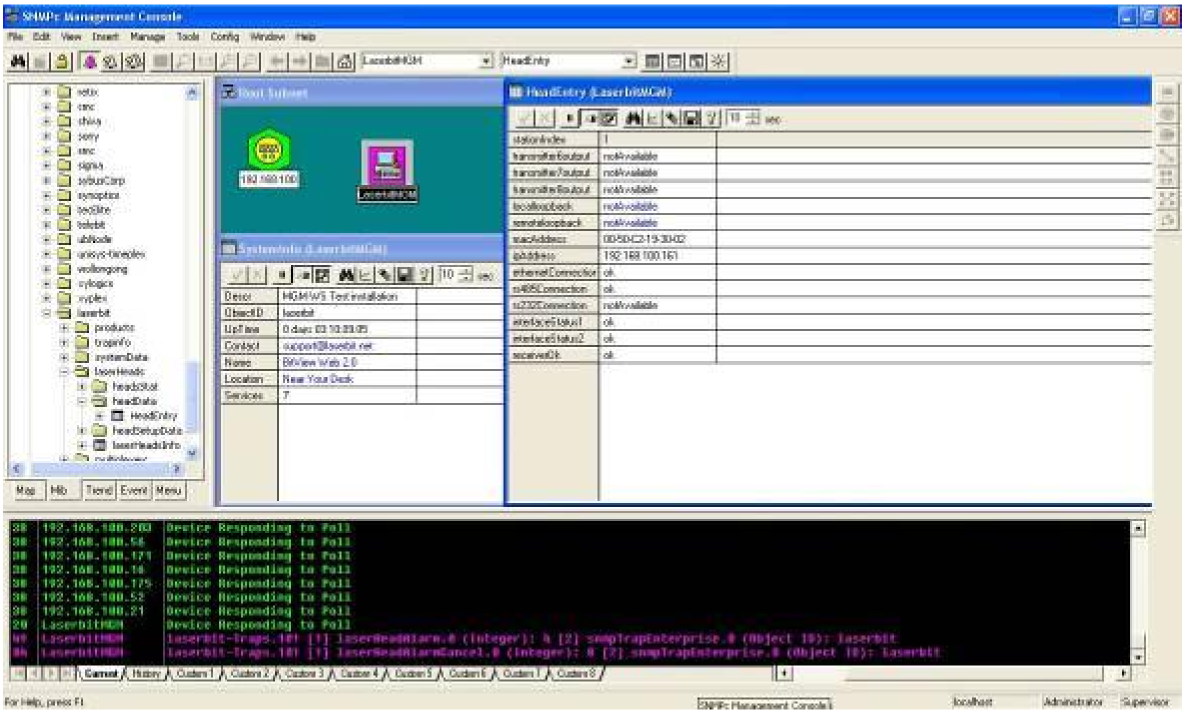
Descr	HGM WS Test installation
ObjectID	laserbit
UpTime	0 days 03:09:34.37
Contact	support@laserbit.net
Name	BitView Web 2.0
Location	Near Your Desk
Services	7

HeadEntry (LaserbitHGM)

stationIndex	1
transmitter1output	notAvailable
transmitter2output	notAvailable
transmitter3output	notAvailable
localloopback	notAvailable
remoteloopback	notAvailable
macAddress	00-50-C2-19-30-02
ipAddress	192.168.100.161
ethernetConnection	ok
rs485Connection	ok
rs232Connection	notAvailable
interfaceStatus1	ok
interfaceStatus2	ok
receiverOk	ok

```
Normal  10/21/2005  10:52:38  192.168.100.207  Device Responding to Poll
Normal  10/21/2005  10:52:38  192.168.100.203  Device Responding to Poll
Normal  10/21/2005  10:52:38  192.168.100.56   Device Responding to Poll
Normal  10/21/2005  10:52:38  192.168.100.171  Device Responding to Poll
Normal  10/21/2005  10:52:38  192.168.100.18   Device Responding to Poll
Normal  10/21/2005  10:52:38  192.168.100.175  Device Responding to Poll
Normal  10/21/2005  10:52:38  192.168.100.52   Device Responding to Poll
Normal  10/21/2005  10:52:38  192.168.100.21   Device Responding to Poll
Normal  10/21/2005  10:58:28  LaserbitHGM      Device Responding to Poll
Minor   10/21/2005  11:00:08  LaserbitHGM      Laserbit-Traps.101 [1] laserHeadAlarm.0 (Integer): 4 [2] snmpTrapEnterprise.0 (Object ID): laserbit
```

After a few seconds the trap message should arrive to your PC.


SNMPc Management Console
File Edit View Insert Manage Tools Config Window Help
LaserbitHGM
HeadEntry
Root Subnet
192.168.100
LaserbitHGM
Map Mib Trend Event Menu
Current History Custom 1 Custom 2 Custom 3 Custom 4 Custom 5 Custom 6 Custom 7 Custom 8
For Help, press F1
SNMPc Management Console
localhost Administrator Supervisor

SystemInfo (LaserbitHGM)

Descr	HGM WS Test installation
ObjectID	laserbit
UpTime	0 days 03:10:33.05
Contact	support@laserbit.net
Name	BitView Web 2.0
Location	Near Your Desk
Services	7

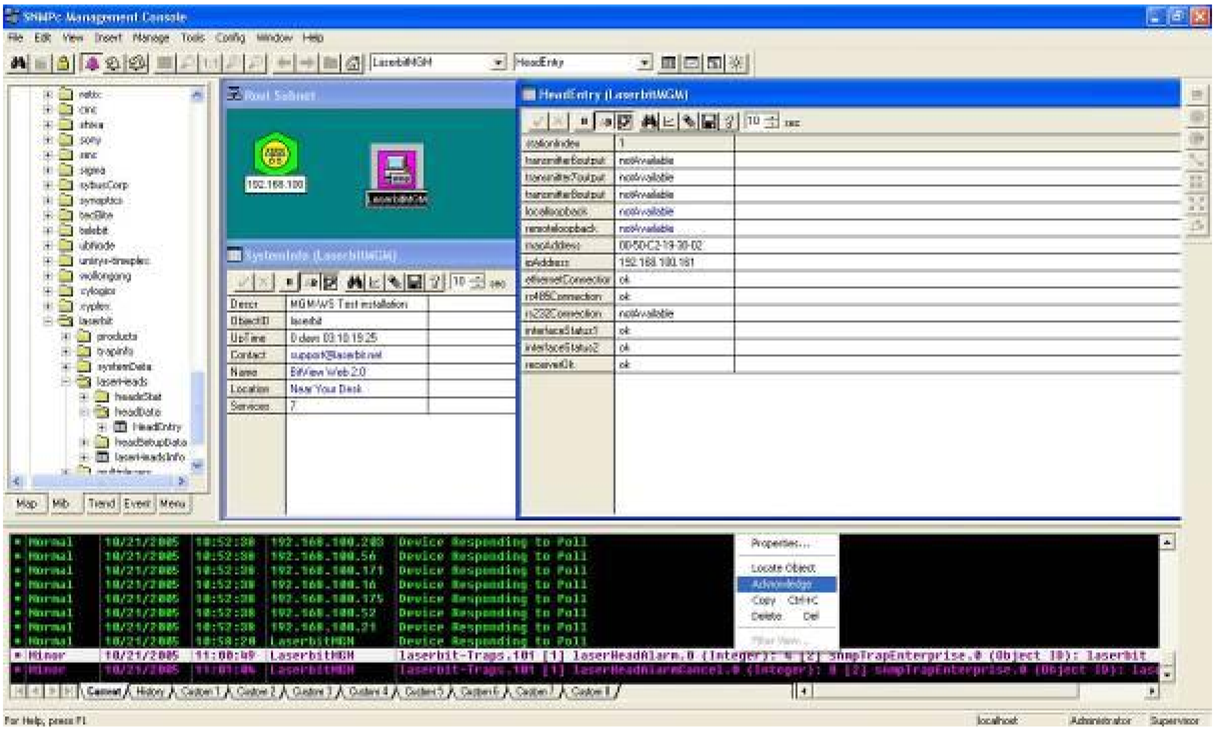
HeadEntry (LaserbitHGM)

stationIndex	1
transmitter1output	notAvailable
transmitter2output	notAvailable
transmitter3output	notAvailable
localloopback	notAvailable
remoteloopback	notAvailable
macAddress	00-50-C2-19-30-02
ipAddress	192.168.100.161
ethernetConnection	ok
rs485Connection	ok
rs232Connection	notAvailable
interfaceStatus1	ok
interfaceStatus2	ok
receiverOk	ok

```
38  192.168.100.203  Device Responding to Poll
38  192.168.100.56   Device Responding to Poll
38  192.168.100.171  Device Responding to Poll
38  192.168.100.18   Device Responding to Poll
38  192.168.100.175  Device Responding to Poll
38  192.168.100.52   Device Responding to Poll
38  192.168.100.21   Device Responding to Poll
28  LaserbitHGM      Device Responding to Poll
08  LaserbitHGM      laserbit-Traps.101 [1] laserHeadAlarm.0 (Integer): 4 [2] snmpTrapEnterprise.0 (Object ID): laserbit
06  LaserbitHGM      laserbit-Traps.101 [1] laserHeadAlarmCancel.0 (Integer): 0 [2] snmpTrapEnterprise.0 (Object ID): laserbit
```

After reconnecting the RS485 cable the trap message should arrive that the alarm was canceled

You can acknowledge the alarm with a right click on the alarm.



Descr	MGM/WS Test installation
ObjectID	laserbit
UpTime	0 days 03:18:19.25
Contact	support@laserbit.net
Name	BitView Web 2.0
Location	Near Your Desk
Services	7

stationIndex	1
transmitter8output	notAvailable
transmitter7output	notAvailable
transmitter8output	notAvailable
localloopback	notAvailable
remoteloopback	notAvailable
macAddress	00-50-C2-19-30-02
ipAddress	192.168.100.181
ethernetConnection	ok
rs485Connection	ok
rs232Connection	notAvailable
interfaceStatus1	ok
interfaceStatus2	ok
receiveOk	ok

```
* Normal  10/21/2005 10:52:38 192.168.100.200 Device Responding to Poll
* Normal  10/21/2005 10:52:38 192.168.100.56  Device Responding to Poll
* Normal  10/21/2005 10:52:38 192.168.100.171 Device Responding to Poll
* Normal  10/21/2005 10:52:38 192.168.100.16  Device Responding to Poll
* Normal  10/21/2005 10:52:38 192.168.100.175 Device Responding to Poll
* Normal  10/21/2005 10:52:38 192.168.100.52  Device Responding to Poll
* Normal  10/21/2005 10:52:38 192.168.100.21  Device Responding to Poll
* Normal  10/21/2005 10:58:20 LaserbitMGM     Device Responding to Poll
* Minor   10/21/2005 11:00:49 LaserbitMGM     laserbit-Traps.101 [1] laserHeadAlarm.0 (Integer): 4 [2] snmpTrapEnterprise.0 (Object ID): laserbit
* Minor   10/21/2005 11:01:06 LaserbitMGM     laserbit-Traps.101 [1] laserHeadAlarmCancel.0 (Integer): 0 [2] snmpTrapEnterprise.0 (Object ID): lase
```

7.4.6 SNMP Technology

SNMP is part of the Internet network management architecture. This architecture is based on the interaction of many entities, as described in the following section.

The Internet Management Model

As specified in Internet RFCs and other documents, a network management system comprises:

Network elements -- Sometimes called *managed devices*, network elements are hardware devices such as computers, routers, and terminal servers that are connected to networks.

Agents -- Agents are software modules that reside in network elements. They collect and store management information such as the number of error packets received by a network element.

Managed object -- A managed object is a characteristic of something that can be managed. For example, a list of currently active TCP circuits in a particular host computer is a managed object. Managed objects differ from variables, which are particular object instances. Using our example, an object instance is a single active TCP circuit in a particular host computer. Managed objects can be scalar (defining a single object instance) or tabular (defining multiple, related instances).

Management information base (MIB) -- A MIB is a collection of managed objects residing in a virtual information store. Collections of related managed objects are defined in specific MIB modules.

Syntax notation -- A syntax notation is a language used to describe a MIB's managed objects in a machine-independent format. Consistent use of a syntax notation allows different types of computers to share information. Internet management systems use a subset of the International Organization for Standardization's (ISO's) *Open System Interconnection* (OSI) *Abstract Syntax Notation 1* (ASN.1) to define both the packets exchanged by the management protocol and the objects that are to be managed.

Structure of Management Information (SMI) -- The SMI defines the rules for describing management information. The SMI is defined using ASN.1.

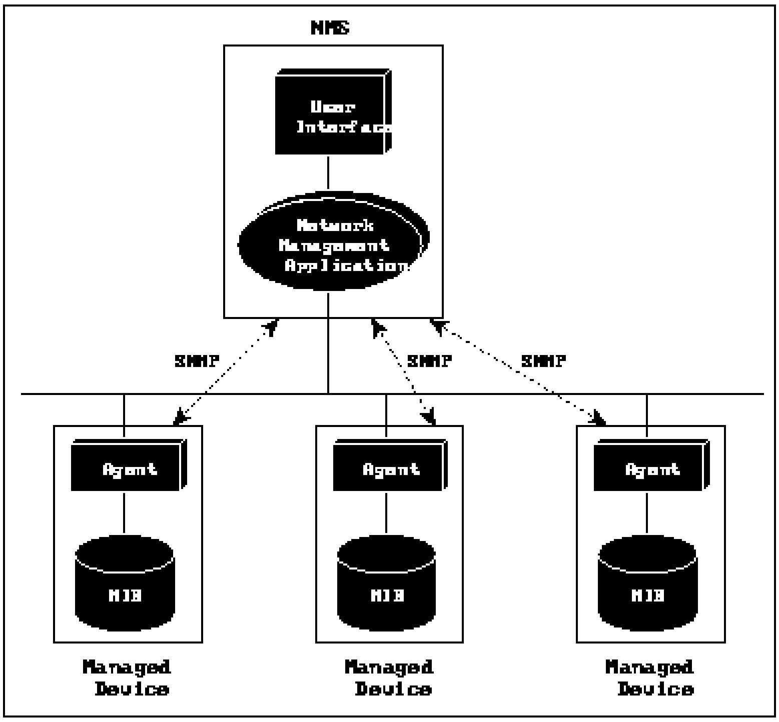
Network management stations (NMSs) -- Sometimes called *consoles*, these devices execute management applications that monitor and control network elements. Physically, NMSs are usually engineering workstation-caliber computers with fast CPUs, megapixel color displays, substantial memory, and abundant disk space. At least one NMS must be present in each managed environment.

Parties -- Newly defined in SNMPv2, a party is a logical SNMPv2 entity that can initiate or receive SNMPv2 communication. Each SNMPv2 party comprises a single, unique party identity, a logical network location, a single authentication protocol, and a single privacy protocol. SNMPv2 messages are communicated between two parties. An SNMPv2 entity can define multiple parties, each with different parameters. For example, different parties can use different authentication and/or privacy protocols.

Management protocol -- A management protocol is used to convey management information between agents and NMSs. SNMP is the Internet community's de facto standard management protocol.

The most basic elements of the Internet management model are graphically represented in *Figure 1*.

Figure 1: The Internet Management Model



Interactions between the NMS and managed devices can be any of four different types of commands:

Reads -- To monitor managed devices, NMSs read variables maintained by the devices
Writes -- To control managed devices, NMSs write variables stored within the managed devices
Traversal operations -- NMSs use these operations to determine which variables a managed device supports and to sequentially gather information from variable tables (such as IP routing tables) in managed devices
Traps -- Managed devices use traps to asynchronously report certain events to NMSs

MIBs and Object Identifiers

A MIB can be depicted as an abstract tree with an unnamed root. Individual data items make up the leaves of the tree. *Object identifiers* (IDs) uniquely identify or name MIB objects in the tree. Object IDs are like telephone numbers -- they are organized hierarchically with specific digits assigned by different organizations.
The object ID structure of an SNMP MIB defines three main branches: Consultative Committee for International Telegraph and Telephone (CCITT), International Organization for Standardization (ISO), and joint ISO/CCITT. Much of the current MIB activity occurs in the portion of the ISO branch defined by object identifier 1.3.6.1 and dedicated to the Internet community.

The current Internet-standard MIB, MIB-II, is defined in RFC 1213 and contains 171 objects. These objects are grouped by protocol (including TCP, IP, *User Datagram Protocol* [UDP], SNMP, and others) and other categories, including "system" and "interfaces."

SMI Definitions

The SMI specifies that all managed objects should have a name, a syntax, and an encoding. The *name* is the object ID, which was discussed in the preceding section. The *syntax* defines the object's data type (for example, "integer" or "string"). A subset of ASN.1 definitions are used for the SMI syntax. The *encoding* describes how the information associated with the managed object is formatted as a series of data items for transmission on the network. Another ISO specification, called the *Basic Encoding Rules* (BERs), details SMI encodings.

SMI data types are divided into three categories: *simple types, application-wide types*, and *simply constructed types*.

Simple types include four primitive ASN.1 types:

Integers -- Unique values that are positive or negative whole numbers, including zero.

Octet strings -- Unique values that are an ordered sequence of zero or more octets.

Object IDs -- Unique values from the set of all object identifiers allocated according to the rules specified in ASN.1.

Bit strings -- New in SNMPv2, these comprise zero or more named bits that specify a value.

Application-wide data types refer to special data types defined by the SMI:

Network addresses -- Represent an address from a particular protocol family.
Counters -- Non-negative integers that increment by positive one until they reach a maximum value, when they are reset to zero. The total number of bytes received on

an interface is an example of a counter. In SNMPv1, counter size was not specified. In SNMPv2, 32-bit and 64-bit counters are defined.

Gauges -- Non-negative integers that can increase or decrease, but latch at a maximum value. The length of an output packet queue (in packets) is an example of a gauge.

Time ticks -- Hundredths of a second since an event. The time since an interface entered its current state is an example of a tick.

Opaque -- Represents an arbitrary encoding. This data type is used to pass arbitrary information strings that do not conform to the strict data typing used by the SMI.
Integer -- Represents signed, integer-valued information. This data type redefines the ASN.1 "integer" simple data type, which has arbitrary precision in ASN.1 but bounded precision in the SMI.

Unsigned integer -- Represents unsigned integer-valued information. It is useful when values are always non-negative. This data type redefines the ASN.1 "integer" simple data type, which has arbitrary precision in ASN.1 but bounded precision in the SMI.

Simply constructed types include two ASN.1 types that define multiple objects in tables and lists:

Row -- References a row in a table. Each element of the row can be a simple type or an application-wide type.

Table -- References a table of zero or more rows. Each row has the same number of columns.

ISO document 8825 (*Specification of Basic Encoding Rules for ASN.1*) defines ISO's BERs. The BERs allow dissimilar machines to exchange management information by specifying both the position of each bit within the transmitted octets and the structure of the bits. Bit structure is conveyed by describing the data type, length, and value.

The SMI for SNMPv2 includes two documents: RFCs 1443 and 1444. RFC 1443 (Textual Conventions) defines the data types used within the MIB modules, while RFC 1444 (Conformance Statements) provides an implementation baseline. The SNMPv2 SMI also defines two new branches of the Internet MIB tree: security (1.3.6.1.5) and SNMPv2 (1.3.6.1.6).

SNMP Operations

SNMP itself is a simple request/response protocol. NMSs can send multiple requests without receiving a response. Six SNMP operations are defined:
Get -- Allows the NMS to retrieve an object instance from the agent.
GetNext -- Allows the NMS to retrieve the next object instance from a table or list within an agent. In SNMPv1, when an NMS wants to retrieve all elements of a table

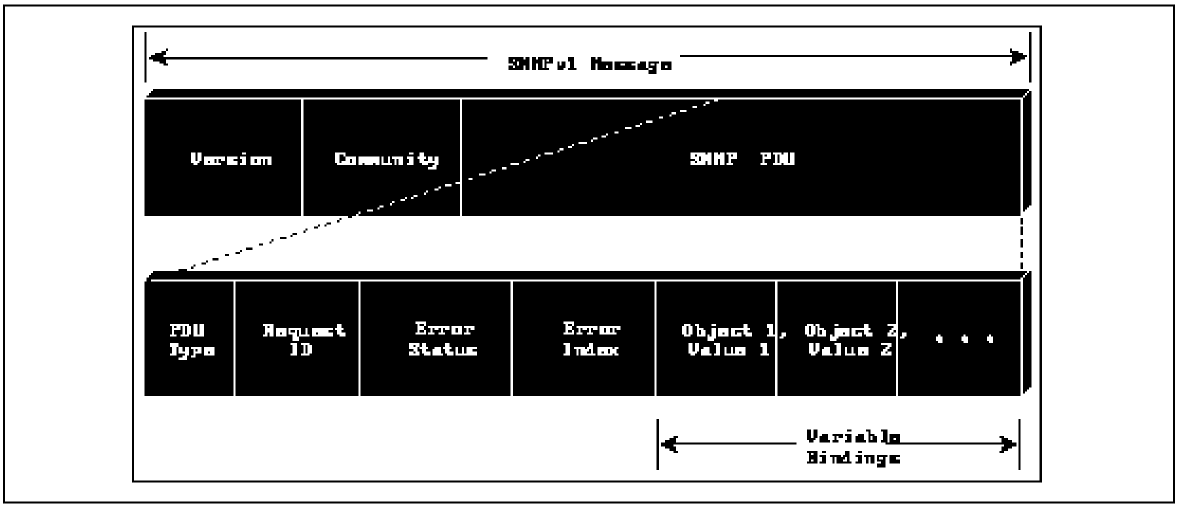
from an agent, it initiates a Get operation, followed by a series of GetNext operations.

GetBulk -- New for SNMPv2. The GetBulk operation was added to make it easier to acquire large amounts of related information without initiating repeated get-next operations. GetBulk was designed to virtually eliminate the need for GetNext operations.

Set -- Allows the NMS to set values for object instances within an agent.
Trap -- Used by the agent to asynchronously Inform the NMS of some event. The SNMPv2 trap message is designed to replace the SNMPv1 trap message.
Inform -- New for SNMPv2. The Inform operation was added to allow one NMS to send trap information to another.

SNMPv1 messages (packets) contain two parts*1*. The first part contains a *version* and a *community name*. The second part contains the actual SNMP protocol data unit (PDU) specifying the operation to be performed ("Get," "Set," and so on) and the object instances involved in the operation. *Figure 3* illustrates the SNMPv1 message format.

Figure 3: SNMP v1 Message Format



* Trap messages have a slightly different format; for information on this format, consult the appropriate SNMP specification.

The version field is used to ensure that all network elements are running software based on the same SNMP version. The community name assigns an access environment for a set of NMSs using that community name. NMSs within the community can be said to exist within the same administrative domain. Because devices that do not know the proper community name are precluded from SNMP operations, network management personnel also have used the community name as a weak form of authentication.

The SNMP PDU has the following fields:

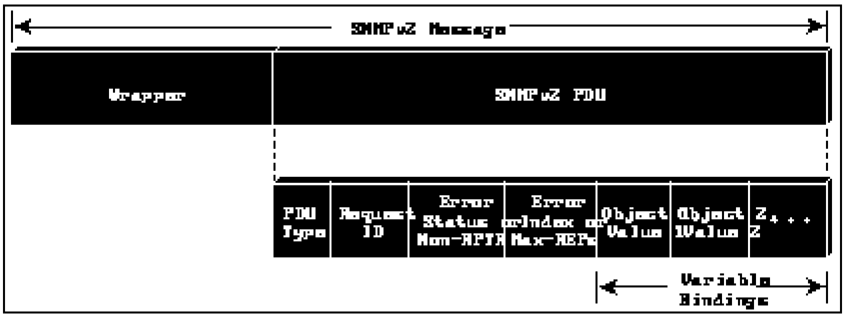
PDU type -- Specifies the type of PDU being transmitted.
Request-ID -- Associates requests with responses.
Error-status -- Indicates an error and an error type. In SNMPv2 GetBulk operations, this field becomes a NonRepeaters field. For these operations, this field defines the number of request-ed variables listed that should be retrieved no more than once from the beginning of the request. The field is used when some of the variables are scalar objects with only one variable.

Error-index -- Associates the error with a particular object instance. In SNMPv2 GetBulk operations, this field becomes a Max Repetitions field. For these operations, this field defines the maximum number of times that other variables beyond those specified by the NonRepeaters field should be retrieved.

Variable-bindings -- Comprises the data of an SNMP PDU. Variable bindings associate particular object instances with their current values.

Like SNMPv1 messages, SNMPv2 messages (shown in *Figure 4*) contain two parts. The second part of the SNMPv2 message (the PDU) is virtually identical to that of an SNMPv1 message (see the previous description of an SNMP PDU for differences). The first part of the SNMPv2 message contains the majority of the differences between SNMPv1 and SNMPv2.

Figure 4: SNMP v2 Message Format



The first part of a SNMPv2 message is often called a *wrapper*. The wrapper includes authentication and privacy information in the form of destination and source parties. As mentioned earlier, a party includes the specification of both an authentication and a privacy protocol. In addition to a destination and a source party, the wrapper includes a *context*. A context specifies the managed objects visible to an operation.
The authentication protocol is designed to reliably identify the integrity of the originating SNMPv2 party. It consists of authentication information required to support the authentication protocol used. The privacy protocol is designed to protect information within the SNMPv2 message from disclosure. Only authenticated messages can be protected from disclosure. In other words, authentication is required for privacy.

The SNMPv2 specifications discuss two primary security protocols: one for authentication and one for privacy. These are the *Digest Authentication Protocol* and the *Symmetric Privacy Protocol.*

The Digest Authentication Protocol verifies that the message received is the same one that was sent. Data integrity is protected using a 128-bit *message digest* calculated according to the Message Digest 5 (MD5) algorithm. The digest is calculated at the sender and enclosed with the SNMPv2 message. The receiver verifies the digest. A secret value, known only to the sender and the receiver, is prefixed to the message. After the digest is used to verify message integrity, the secret value is used to verify the message's origin.

To help ensure message privacy, the Symmetric Privacy Protocol uses a secret encryption key known only to the sender and the receiver. Before the message is authenticated, this protocol uses the *Data Encryption Standard* (DES) algorithm to effect privacy. DES is a documented *National Institute of Standards and Technology* (NIST) and *American National Standards Institute* (ANSI) standard.

Originally, SNMPv1 specified that SNMP should operate over the *User Datagram Protocol* (UDP) and IP. The SNMPv2 transport mapping document (RFC 1449) defines implementations of SNMP over other transport protocols, including *OSI Connectionless Network Service* (CLNS), AppleTalk's *Datagram Delivery Protocol* (DDP), and Novell's *Internet Packet Exchange* (IPX). RFC 1449 also includes instructions on how to provide a SNMPv1 proxy and use of the BER. UDP/IP is still SNMPv2's preferred transport mapping because UDP is compatible with SNMPv1 at both the transport and network layers.

Trap event list

Alert disabled: there is no alert coming up for this trap
Temperature: The agent will send an alarm if the value goes above the preset value. For further details please see *Temperature alert level in the **Device Setup*** chapter.
Detector: The agent will send an alarm if the value goes above the preset value. For further details please see *Detector alert level in the **Device Setup*** chapter.
Transmitter: if the transmitter fails operating the agent will send an alarm.
Power supply: if the power supply reports fault the agent will send the alarm.
Receiver: If the receiver gets into disabled the agent will send an alarm. For further details please see *RX OK* in the ***Status info screen*** chapter
Remote Failure: If the local head loses the connetion to the remote head the agent will send an alarm. For further details please see *Remote is visible* in the ***Status info screen*** chapter
FSO Link:The Agent will send an alarm if the valid signal is lost. . For further details please see *FSO Link* in the ***Status info screen*** chapter.
TP Link: The Agent will send an alarm if the connection is lost on the local TP port. For further details please see *TP_Link* in the ***Status info screen*** chapter.
Traffic error: The agent will send an alarm if any of the values on the *Network statistics page* is incremented.

8 Warranty conditions

GeoDesy FSO (Europe) LTD warrants that the **GeoDesy FSO** product purchased will free from defects in material and workmanship for a period of one (1) year from the date of purchase. This warranty period will not be extended by virtue of a repair of the product or a replacement of any component of the product during the warranty period.

This warranty covers only normal commercial use. **GeoDesy FSO (Europe) LTD** is not responsible for warranty service should the **GeoDesy FSO** identification marks, serial numbers or original seals be removed, altered, or broken, or should the product fail to be properly maintained or fail to function properly as a result of any modification, misuse, abuse, improper installation, neglect, improper shipping, damage caused by disasters such as fire, flood, earthquake or lightning, improper electrical current, or service other than by **GeoDesy FSO (Europe) LTD** or its authorised partners.

If the **GeoDesy FSO** product fails to operate as warranted at any time during the warranty period, **GeoDesy FSO (Europe) LTD** will repair, or at its option, replace the defective product at no additional charge.

In no event will **GeoDesy FSO (Europe) LTD** be liable for any damages including loss of data, lost profits, lost savings, lost business, or other incidental or consequential or indirect damages arising out of the installation, use, maintenance, performance, failure or interruption of the **GeoDesy FSO** product, even if **GeoDesy FSO** (Europe) LTD has been advised of the possibility of such damage.

If you purchased the **GeoDesy FSO** product in the United States, some states do not allow the limitation or exclusion of liability for incidental or consequential damages, so the above limitation may not apply to you.

The purchaser or user shall have the responsibility to give **GeoDesy FSO (Europe) LTD** prompt written notice of any warranty claims. If the product was purchased through an authorised partner of **GeoDesy FSO (Europe) LTD**, notice may be given in writing to that authorised partner in the area in which the product was being used.

The product may be returned to **GeoDesy FSO (Europe) LTD** only if it has a Return Material Authorisation (RMA) number. The product must be shipped prepaid, insured and in the original shipping package or similar package for safe shipment. The RMA number must be marked on the outside of the shipping package. Any product returned without an RMA number shall be rejected.

Transportation charges for the return of the product will be paid by **GeoDesy FSO (Europe) LTD** if it is determined by **GeoDesy FSO (Europe) LTD** that the product was defective within the terms of the warranty; otherwise the purchaser or user shall be responsible for costs of return handling and transportation.

If the **GeoDesy FSO** product does not operate as warranted above, the customer's sole remedy shall be repair or replacement. The foregoing warranties and remedies are exclusive and are in lieu of all other warranties, expressed or implied, either in fact or by operation of law, statutory or otherwise, including warranties of merchantability and fitness for a particular purpose. **GeoDesy FSO** neither assumes nor authorises any other person to assume for it any other liability in connection with the sale, installation, use or maintenance of the product.

9 Privacy statement

We will never share, sell, or rent individual personal information with anyone without your advance permission or unless ordered by a court of law. Information submitted to us is only available to employees managing this information for purposes of contacting you or sending you emails based on your request for information and to contracted service providers for purposes of providing services relating to our communications with you.